

## **The paradox of Corporate fraud-victimless yet pervasive!**

**(Vandana Singh<sup>1</sup>)**

Economic crime and fraud are a reality that all organizations no matter what their size are confronted. Fraud is often dismissed as a corporate or victimless crime and much of it remains hidden. But the reality is that everyone is at risk and the threat is increasing with advances in the digital arena and the growth of the Internet. In fact the range and scale of fraudulent activity makes it more and more difficult to get an accurate overview of its overall economic and emotional impact, especially as large amounts of fraud remain unreported.

### **Defining Fraud and Identifying perpetrators**

Fraud essentially involves using deception and concealment to make a personal gain for oneself and/or create a loss for another dishonestly. Generally, the term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.<sup>2</sup> Fraud as “deception or misrepresentation that an individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual or to the entity or some other party”<sup>3</sup> is a deliberate act which has over the past few decades been the top concern for the corporate executives.

According to the Contract Act, 1872, ‘fraud means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with an intent to deceive another party thereto or his agent, or to induce him to enter into the contract: (1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true; (2) the active concealment of a fact by one having knowledge or belief of the fact; (3) a promise without

---

<sup>1</sup> Assistant Professor, Dr. Ram Manohar Lohiya National Law University, Lucknow-226006

<sup>2</sup> Stephen Hill, *Corporate Fraud: Prevention and Detection*, (Second Edition), Bloomsbury Professional Ltd, London, 2010, P.2.S

<sup>3</sup> Fraud as defined by the Association of Certified Fraud Examiners (ACFE)

any intention of performing it;(4) any other act fitted to deceive; (5) any such act or omission as the law specially declares to be fraudulent.

The term fraud has been defined in the Companies Act, 2013 in the *Explanation* to section 447 which defines and prescribes punishment for frauds. There is a corresponding provision in the 1956 Companies Act. One relevant *Explanation* to the section 447 containing the definition of fraud is as follows: ‘fraud’ in relation to affairs of a company or any body corporate includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.

Corporate fraud means the fraud that affects companies, businesses and other similar organizations which may manifest in frauds committed by the top levels of management, such as the Board of Directors including not just direct misappropriation of the funds but also accounts manipulation; frauds committed by employees apart from the top management including ‘selling on’ of stock and siphoning off of money from business to personal accounts; and external fraud. A high percentage of frauds are committed by senior management (including owners and executives), average losses caused by owners and executives being nearly 12 times those of employees, and losses caused by managers are generally more than double those caused by the employees.<sup>4</sup>

Fraud can be undertaken by anyone and it is usually those we least suspect. When frauds are discovered, there is often shock and disbelief that they could have committed such an act. The perpetrator of business fraud could be ‘the person next door.’ Typically, a fraudster is a very ambitious mid-management employee, far from retirement, working in the procurement or sales department, says consultancy firm Ernst & Young India Report titled ‘*Fraud and corporate governance: changing paradigm.*’ Ranging from an individual carrying out a one-off activity for personal gain, to highly organized operations siphoning large amounts of money to fund other criminal activity, fraud is an area where we are all affected and indeed victims. Commonly

---

<sup>4</sup> ACFE’s 2008 *Report to the Nation*, a research on frauds committed in the US and KGMP researched *Profile of a Fraudster*(2007) in Europe, India, the Middle East and South Africa.

known as the ‘silent crime’, fraud affects the lives of many, with most of us not realizing we are victims until we apply for credit or have court summons issued against us.

### **Impulsion to Fraud**

While researching his doctoral thesis in 1950s, famed criminologist Donald R Cressey came up with the ‘fraud triangle’, a hypothesis to explain why people commit fraud. The three key elements in the fraud triangle are opportunity, motivation and rationalization. The opportunity to commit fraud is possible when employees have access to information/ data, for example that allows them to both commit and conceal a fraud. Motivation, another aspect of the fraud triangle, is a pressure or a ‘need’ felt by the person who commits fraud. It could be a real or a perceived financial need or even a non-financial need for instance high pressure for good results at work or a need to cover up someone’s poor performance. Finally, employees may rationalize this behavior by determining that committing fraud is okay as they are making up for being underpaid or replacing a bonus that was deserved but not received. Some embezzlers tell themselves that the Company does not need the money or will not miss the assets.<sup>5</sup> In many cases the offender has “little or no criminal self-concept and offenders view violation as part of their work.”<sup>6</sup> Further they usually minimize their crime since it results in minor losses for a large volume of clients; no one client is usually targeted for the crime. In most cases, offenders do not view stealing from companies as harmful; they may think that the crime was victimless; and they do not view their theft as being devastating or costly to the business.

### **Shades of Corporate Fraud**

Corporate fraud generally falls into one of the three categories; asset misappropriation, corruption and financial statement fraud.

The first and by far the most common category is asset misappropriation, cash or non-cash-essentially, stealing-which includes larceny (i.e., after the asset is recorded on the books) and skimming (i.e., before the asset is recorded on the books).

---

<sup>5</sup>Stephen Hill, *Corporate Fraud: Prevention and Detection*, (Second Edition), op.cit., p.4

<sup>6</sup> Frank E Hagan, *Introduction to Criminology: Theories, Methods and Criminal Behavior*, 4<sup>th</sup> edition, 1997, p.319.

Corruption is frequently perceived as the way of doing business in India, India ranking 94 out of 176 countries/territories as per Transparency International's Corruption Perception Index of the year 2012. The extremely competitive and challenging conditions in which the businesses operate today with several unstable markets, sluggish or minimal growth in others and an aggressive enforcement environment around the world, corruption and bribery are pervasive in nature and there is a high level of organizational tolerance for the vice. The common manifestations of corruption include activities that characterize conflict of interests, bribery, economic extortion and kickbacks.

The ACFE defines financial misstatement as deliberate misrepresentation of the financial condition of an enterprise. This is accomplished through intentional misstatement or omission of accounts or disclosures in its financial statements to deceive users.<sup>7</sup> A fraud survey of the year 2013 conducted by EY's EMIEA reveals that executives and their teams are under increasing pressure to deliver unrealistic results in difficult markets. Around 74% of Indian managers agree that they are under pressure to deliver a good financial performance over the next 12 months.<sup>8</sup> Alarming, a large number of the respondents in the survey appeared to be comfortable with or even aware of the unethical conduct in their organizations including recording revenues too early, under-reporting costs or encouraging customers to buy unnecessary stock, yet looked the other way in their quest to grow and improve their performance. Increased revenues without a corresponding increase in cash flow, especially over time, strong revenue growth when peer companies are experiencing weak sales and significant, unusual or highly complex transactions, particularly those that are closed near the end of a financial reporting period are some red flags ACFE has listed to identify financial fraud schemes.

Within these broad categories can be included payroll frauds such as overstatement of wages, showing payments of perquisites which have not been provided, claiming overtime, no disbursement done; inflating day-to-day expenses; frauds concerning dealings with vendors such as over-pricing, paying for goods never received/received in a damaged condition; frauds concerning investments; frauds relating to customers; billing frauds; tampering with cheques and electronic transfers; reimbursements shown which have never been made; frauds concerning

---

<sup>7</sup>The 2007 Annual Association of Certified Fraud Examiners Manual.

<sup>8</sup>*Navigating today's complex business risks*, Ernst & Young's EMEIA Fraud Survey 2013.

cash register disbursements; misuse of the properties of company, confidential information, patents, copyrights; misappropriation of securities such as treasury bills or company's stocks or investments in companies from where money invested could never be recovered.<sup>9</sup>

Since human ingenuity is limitless, the list would be bound to be further augmented. Cybercrime, intellectual property infringement including counterfeiting and piracy, and identity theft (either by way of password sharing, social engineering or malwares) are rated as the top fraud concerns for the future by the *KPMG India Fraud Survey 2012*.<sup>10</sup> This underlines a shift in the fraud landscape with fraudsters increasingly targeting organizational knowledge (data, code etc) and not physical assets to defraud companies. These futuristic frauds rely on technology and allow fraudsters to work in groups to leverage their full might leaving all companies vulnerable irrespective of size, sector and operations. Information illegally copied/ taken from a business or other individual or data theft involves the fraudster accessing customer details and financial data, including credit card numbers, bank accounts details, trade secrets, pricing information, sales data, marketing information, intellectual property, formulae, research, software source code and algorithms, system and user credentials, such as passwords and certificates.

There have been many attempts to measure the extent of fraud, but it is not easy to compile reliable statistics. One of the key aspects of fraud is deception, so fraud can be difficult to identify. Often survey results reflect only the instances of fraud that have actually been discovered. It is estimated that the majority of frauds go undetected. Some frauds may not be reported even when they are found. It is also often hard to distinguish fraud from carelessness and poor record keeping. Thus the cost of fraud to businesses is difficult to estimate because not all fraud and abuse is discovered, not all uncovered fraud is reported, and civil or criminal action is not always pursued. The reason the companies don't talk about it is that it shows them in poor light. Who wants stakeholders to know about illicit deals, siphoning off funds and information leaks? Apart from direct economic loss to business, legal, accounting & increased insurance costs, and loss of productivity associated with hiring and firing employees, are additional factors that must be considered.

---

<sup>9</sup>T.N.Pandey, Corporate Frauds-Nature, Control and Regulation, *SEBI and Corporate Laws*, June 15-June 30, 2014, Vol.125, Issue 4, p.110.

<sup>10</sup> The KPMG Fraud Survey received responses from 293 CXOs representing Indian and multinational firms from varied industries across Financial Services, Information and Entertainment, Industrial markets, Real Estate & Infrastructure, Consumer Markets, Telecom, Travel Tourism and Leisure, Healthcare & Social Sector.

Corporate frauds worth more than Rs 10,800crore have been detected by Investigation Agency SFIO during its probe in 78 cases nearly three-and-half years from 2011-12 till June end 2014.<sup>11</sup>

### **Mitigating Fraud Risks**

A one-size-fits-all framework cannot help mitigate emerging fraud risks because each risk manifests itself uniquely. Only when the companies are aware of the various possible modus operandi, perpetrators and gaps in internal controls can they evolve an effective risk-mitigation framework. Comprehensive information security measures, protection of personal information, physical security measures and robust access protocols along with periodic reviews can be adopted to tackle frauds holistically. There are two main elements to fraud prevention:

1. A sound ethical culture.
2. Sound internal control systems.

**Developing a sound ethical culture:** In order to establish a sound ethical culture, it is recommended that organizations have:

1. A mission statement that refers to 'quality' or 'ethics' and defines how the organization wants to be regarded externally.
2. Clear policy statements on business ethics and anti-fraud, with explanations about acceptable behavior in risk-prone circumstances.
3. Management which is seen to be committed through its actions.
4. Fraud risk training and awareness for all employees and key business partners.
5. A process of reminders about ethical and fraud policies, for example, an annual letter and/or declarations.
6. Periodic assessment of fraud risk.
7. A route through which suspected fraud can be reported.
8. An aggressive audit process which concentrates on fraud risk areas.

**Sound internal control systems:** An internal control system comprises all those policies and procedures that collectively support an organization's operation. Internal controls typically deal with approval and authorization processes, access restrictions, transaction controls, account

---

<sup>11</sup>*The Economic Times*, Corporate frauds of Rs 10,800 crore detected by SFIO, July 26, 2014.

reconciliations and physical security. These procedures often include the division of responsibilities, and checks and balances to reduce risk.<sup>12</sup>

The number and type of internal controls that an organization can introduce depends on its nature and size. Although fraud is prevalent across organizations of all sizes, sectors and locations, research shows that certain business models have greater levels of fraud risk than others. The control environment should be adjusted to fit with the degree of risk exposure. Wherever possible, internal controls should address warning signs and alerts to minimize fraud.

However, the reality is as happened in the case of the Rs7000 crore accounting fraud at Satyam—the prevalence of collusion, conspiracy and fraud in general. If people want to perpetrate a certain fraud and there's collusion involved, there isn't a mechanism in place to necessarily detect it.

### **Evolving Regulatory Landscape**

The Companies Act 2013 seeks to introduce significant changes in corporate governance standards in India as it aims to deter corporate crime and related offences in diverse ways. The Satyam scandal, the biggest fraud at a listed company in India which cost shareholders more than \$2bn and rocked India's IT industry, brought into sharp focus, the importance of securities laws and Corporate Governance in emerging markets. Indeed, Satyam fraud spurred the government of India to tighten the CG norms to prevent recurrence of similar frauds in future. The new Companies Act aims to make the Serious Fraud Investigation Office (SFIO), a powerful agency for investigating corporate fraud. Statutory status will be conferred on this body with powers to arrest individuals for certain offences that attract punishment for fraud. For speedy prosecution in matters or cases investigated by the SFIO, the investigation report of this agency filed with the special court will be deemed as a report filed by a police officer. Stringent penalties are prescribed for fraud-related offences.<sup>13</sup> A Market Research and Analysis Unit (MRAU) has been set up in SFIO to analyze media reports relating to financial frauds and for conducting market surveillance of such corporates.

---

<sup>12</sup>[http://www.cimaglobal.com/documents/importeddocuments/cid\\_tg\\_corporate\\_fraud\\_may09.pdf](http://www.cimaglobal.com/documents/importeddocuments/cid_tg_corporate_fraud_may09.pdf)

<sup>13</sup>*Deterrence and detection of financial fraud. A growing concern.* A report by Fraud Investigation & Dispute Services, Ernst & Young LLP, p.14.

Additionally, clause 177(9) of the Act mandates every listed company to establish a vigil mechanism for directors and employees to report genuine concerns in the manner prescribed along with provision of adequate safeguards against victimization of whistle-blowers.<sup>14</sup> The Act also expands the responsibility on auditors who will face criminal liability if they fail to report corporate fraud within a stipulated time frame. This indirectly makes them responsible for functioning of the vigil mechanism within the company. The vigilance mechanism has to be duly displayed on the company website and its activities reported in annual report. The new Act has also introduced the concept of class action suit wherein the depositors or a unit of shareholders can sue a firm that has committed fraud.<sup>15</sup>

The Act outlines the duties and responsibilities of Independent Directors to prevent and report fraud, making the IDs responsible for enhanced internal controls, strong governance and efficient whistle-blowing mechanisms at companies on whose boards they preside. It directs them to uphold ethical standards of integrity and probity and satisfy themselves about the integrity of financial information provided to them and the robustness of the company's financial controls and systems of risk management. Additionally, the Act mandates that they report their concerns about unethical behavior and actual or suspected fraud or violation of a company's code of conduct or ethics policy.<sup>16</sup> Section 447 of the Act for the first time provides specifically, punishment for frauds both in physical (imprisonment not less than six months extendable to ten years in non-public interest cases and not less than three years in fraud involving public interest) and monetary terms (fine not less than the amount involved in the fraud which might extend to three times the amount involved in fraud).

The Act thus balances external and internal forces to significantly improve corporate governance and bring into its fold, the liabilities of responsible parties and the interests of various stakeholders.

The National Financial Reporting Authority (NFRA), a quasi-judicial body under the new Companies Act shall be the apex body for accounting and auditing standards, with powers to probe and review audits of companies, including those which have securities listed outside India

---

<sup>14</sup> Ibid.

<sup>15</sup> *The Economic Times*, Historic feat: Parliament passes new Companies Bill, August 06, 2013.

<sup>16</sup> *Deterrence and detection of financial fraud. A growing concern.* A report by Fraud Investigation & Dispute Services, Ernst & Young LLP, po.cit.

according to draft rules issued by the Corporate Affairs Ministry. NFRA has the responsibility of monitoring, compliance review and overseeing quality of service, enforcement and standard setting with regard to accounting and auditing standards. In addition, NFRA would have the authority to conduct investigation on reference made by the central government or any regulator. It can also *suomotostart* investigation in public interest. Further, NFRA can undertake peer review/investigation of auditors or audit firms which conduct audit of 200 companies or more in a year as well as those auditing 20 or more listed entities. The penalties on audit firms by NFRA can be very severe, and include debarment of an audit firm for a maximum period of 10 years. The NFRA will prepare once in every year an annual report giving a true and full account of its activities performed in the year, including the results of its various monitoring activities.<sup>17</sup>

Faced with a growing number of financial frauds, the Corporate Affairs Ministry has set up a new intelligence unit that will delve into 'data mining' from all possible sources to detect any wrongdoings by the companies and their promoters at the earliest possible stage. The idea is to have a set of people to do the data mining, collection and checking of records that is available on various platforms, and then link them with the inputs from investigating agencies.<sup>18</sup>

The previous Congress government also undertook several measures to protect the investor interests through programs on awareness and education. Some of these steps include issues of multi-lingual print media advertisements from time to time to caution the investors about fraudulent investment schemes, creation of facility on MCA-21 website for lodging complaints and for tracking their status and a system of sending SMSes cautioning investors to be careful while making investments.<sup>19</sup> The Ministry of Corporate Affairs ordered probe in 139 cases of alleged corporate fraud through Serious Fraud Investigation Office (SFIO) by December 2013 involving allegations of siphoning off/diversion of funds by the promoters/directors, manipulation of books of accounts through running of pyramidal schemes and misuse of collective investment schemes by companies for collecting money from the public.<sup>20</sup>

---

<sup>17</sup>*Economic Times*, NFRA to get powers to investigate companies, audit firms, Oct 22, 2013

<sup>18</sup>*Times of India*, New intelligence unit to detect corporate frauds: Govt. Dec 30, 2012

<sup>19</sup>*The Economic Times*, SFIO asked to probe 125 companies for defrauding investors in 4 years, August 22, 2013.

<sup>20</sup>*The Economic Times*, No instance of Satyam-like fraud seen in any other company so far, says government, December 12, 2013.

India's capital market regulator SEBI has formed a separate team to detect financial or corporate frauds in a bid to beef up its investigation process. The new unit called Forensic Accounting Cell will be a part of the Securities and Exchange Board of India's corporate finance department that will aim at creating a mechanism to warn against corporate scandals. SEBI has set up the unit in the wake of increasing complaints against companies by investors accusing them of rigging financial statements.<sup>21</sup>

Come October 1, 2014, as per Securities and Exchange Board of India's Listing Agreement, all listed companies have to mandatorily have a whistleblower policy under Clause 49 and also put in place, a vigil mechanism to report concerns on unethical behavior, actual or suspected fraud or violation of the company's code of conduct or ethics policy by employees and directors to the management.<sup>22</sup>

### **Detriments to deterrence**

The best way to reduce the occurrence of fraud is strengthening the internal control systems assigning an increasingly significant role to the auditors. In India, Clause 49 of SEBI's Listing Agreement provides for regulations to maintain internal controls over financial reporting. However, their effectiveness is evaluated by the Audit committee and not by any supreme oversight body (as the Public Company Accounting Oversight Board mandated by the Sarbanes Oxley Act in the United States). Also Clause 49 does not elaborate internal control or the underlying documentation framework required leaving the responsibility of establishing, maintaining and evaluating internal control to the Chief Executive Officer or the Chief Financial Officer. Neither does it elaborate internal control framework as a mandatory requirement leading to the increased tendency amongst the companies to comply with the bare minimum requirement. A propensity to neglect the internal audit wing, posting the comparatively less competent, inexperienced, untrained & unskilled personnel therein is also witnessed. Consequently, companies are geared up to detect errors rather than deterring frauds.<sup>23</sup>

Indian companies are defensive when it comes to reporting fraud. Even when the management of the vigil mechanism is managed by third-party external agencies, the results have not been

---

<sup>21</sup>*The Economic Times*, Sebi sets up a separate cell to detect corporate frauds, Reena Zachariah, February 23, 2012.

<sup>22</sup>*Business Standard*, Sudipto Dey, Why India Inc is defensive when it comes to reporting frauds, June 02, 2014.

<sup>23</sup>*Business Line*, Deterring Corporate Fraud, June 19, 2011.

encouraging. The propensity of an overwhelming percentage of the complainants to remain anonymous results in many companies ignoring these complaints. Whistle blowing being at a nascent stage in India is mostly used as a “good to comply with” measure. A serious gap in the current legislative mechanism is that Indian regulations are limited to employees and directors of the company leaving out vendors and suppliers. Also, the government should prescribe what constitutes “adequate” safeguards to protect victimization of whistleblowers instead of leaving it to the company to devise its own vigil mechanism. For the vigil mechanism to be effective, companies need to encourage whistle blowing as a part of corporate culture and work ethics along with a reward system to encourage whistle blowing and regular external audits of the vigil mechanism to inspire confidence in the system.<sup>24</sup>

### **Conclusion-Securing against fraud risks**

An organization’s approach to dealing with fraud should be clearly described in its fraud policy and fraud response plan. The plan should provide procedures which allow for evidence gathering and collation. A fraud response plan should thus include definition of fraud, information regarding purpose of the fraud response plan, the actual response, the investigation, organization’s objectives with respect to dealing with fraud and follow up action. The fraud response plan should reiterate the organization’s commitment to high legal, ethical and moral standards in all its activities, and its approach to dealing with those who fail to meet those standards. Organizations should be clear about how to enforce the rules or controls which are in place to counter fraud risks. They must also ensure that employees know how to report suspicious behavior.

The organization’s willingness to learn from every identified fraud experience is as important as any other response. Organizations should examine the circumstances and conditions which allowed the fraud to occur, with a view to improving systems and procedures so that similar frauds do not recur. Fraud detection acts as a deterrent by sending a message to likely fraudsters that the organization is actively fighting fraud and that procedures are in place to identify any illegal activity. The possibility of being caught will often persuade a potential perpetrator not to commit a fraud. There should also be complementary detection to counter the fact that the

---

<sup>24</sup>*Business Standard*, Sudipto Dey, Why India Inc is defensive when it comes to reporting frauds, June 02, 2014.

prevention controls may be insufficient in some cases. It is also important to have a consistent and comprehensive response to suspected fraud incidents. This sends a message that fraud is taken seriously and that action will be taken against perpetrators.

A tailor-made anti-corruption training program for employees and selected third parties can proactively help in setting the proper tone in an organization. The use of efficient IT tools such as e-discovery and forensic technology helps organizations continuously monitor their business transactions & communications and also retrospectively identify fraudulent payments or other such activity. And finally, the regulators should ensure that the corporate put in place, a strong whistle blowing arrangement as part of their strategic agendas and adequate internal control systems to ensure effectiveness of controls and monitoring over financial reporting attested by an independent auditor to mitigate possibility and opportunity for fraud by fudging financial statements, a recurrent theme in corporate fraud.

With the ever-changing and complex nature of frauds, no system can be a hundred percent secured from unknown threats but a certain level of preparedness can go a long way in countering fraud risks, limiting damages and protecting the reputations of organizations. Concerted risk-focused efforts targeting areas of exposure can enable companies to appropriately balance their priorities of growth and ethical business conduct while seizing opportunities in the present competitive fraud-fraught corporate landscape. With a court in Hyderabad pronouncing B. Ramalinga Raju, the founder of Satyam Computer Services (and nine others under various sections of IPC) guilty of forging documents and falsifying accounts thus sentencing him to seven years in prison, it is anticipated that the long awaited judgment given by the court will have far reaching consequences in checking corporate frauds and shall also act as a severe deterrent.

**\*Dr. Vandana Singh,**

**Assistant Professor (History),**

**Dr. Ram ManoharLohiya National Law University, Lucknow.**

**Mobile: 09452235942**

**e-mail:vandanasingh06@yahoo.co.in**

Dear Sir/Madam,

I am mailing my Research Paper titled '**The Paradox of Corporate fraud-victimless yet pervasive**' in response to your call for papers. Kindly apprise me of the status of the paper as early as the procedures permit.

Sincerely

Vandana Singh,

Assistant Professor,

Dr. Ram ManoharLohiya National Law University, Lucknow-226006

Mobile: 09452235942

e-mail: vandanasingh06@yahoo.co.in