Australian Journal of Business and Management Research
New South Wales Research Centre Australia *(NSWRCA)*

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

MENACE OF FRAUDS IN THE INDIAN BANKING INDUSTRY: An Empirical Study

Dr. Madan Lal Bhasin
Visiting Professor, School of Accountancy
College of Business
Universiti Utara Malaysia (UUM), Kedah, Malaysia
madan.bhasin@rediffmail.com

ABSTRACT

Banks are the engines that drive the operations in the financial sector and growth of an economy. With the growing banking industry in India, frauds in Banks are also increasing and fraudsters are becoming more sophisticated and ingenious. While it is not possible for Banks to operate in a zero fraud environment, proactive steps such as conducting risk assessments of procedures and policies can help them hedge their risk of contingent losses due to fraud. Thus, time has come when the security aspects of the Banks have to be dealt with on a priority basis. As part of the study, a questionnaire-based survey was conducted in 2012-13 among 345 Bank employees "to know their perception towards bank frauds and evaluate the factors that influence the degree of their compliance level." This study reveals that "there are poor employment practices and lack of effective employee training; usually over-burdened staff, weak internal control systems, and low compliance levels on the part of Bank Managers, Offices and Clerks. However, technology can play a major part in combating new-age frauds: proactive forensic data analysis and data mining techniques can help governments, regulatory bodies and Banks to counter the increasingly complex nature of frauds.

Keywords: *Bank frauds, public-sector banks, India, banking industry, RBI, internal controls, risk management, use of technology.*

Introduction

A well-organized and efficient banking system is an essential pre-requisite for overall economic growth of every country. Banking industry plays an important role in the functioning of organized money markets, and also acts as a conduit for mobilizing funds and channelizing them for productive purposes. But it has been observed during the last 50 years that even the sophisticated markets and long-functioning banking systems have had significant bank failures and bank crisis on account of increasing magnitude of frauds. According to the Association of Certified Fraud Examiners' (ACFE, 2012) 'Report to the Nations,' "the cost of fraud to the US organizations is extensive—5 percent of annual revenues, despite increased emphasis on anti-fraud controls and recent legislation to combat fraud." Indeed, bank failures are a direct threat to the economy of any country, and hence, urgent regulatory changes are required to be designed to decrease the probability of future bank failures and lessen the cost of bank failures. Fraud detection in banking industry is a critical activity that can span a series of fraud schemes and fraudulent activity from bank employees and customers alike. Banks, therefore, need to get their customers actively involved in their fraud prevention efforts as customers may be willing to switch to competing banks if they feel left in the dark about those efforts. Thus, banking industry's risk mitigation and fraud prevention efforts must support a financial institution's strategic goals of increasing customer satisfaction and contributing additional revenue—all while protecting customers and the organization's reputation. Since banking industry is a highly-regulated industry, there are also a number of external compliance requirements that banks must adhere to in the combat movement against fraudulent and criminal activity.

Banking industry in India has traversed a long-way to assume its present stature in the 21st century. It has undergone a major structural transformation after the nationalization of 14 major commercial banks in 1969, and 6 more in 1980. The Indian banking system is unique and has no parallels in the banking history of any country in the world. Indian's banking system has several outstanding achievements to its credit, the most striking of which is its wide and easy reach. In fact, Indian banks are now spread out into the remotest areas of our country. The Indian banking industry, which was operating in a highly comfortable and protected environment till 1990s, has been pushed into the choppy waters of intense competition. After Independence, the banks have passed through three stages. They have moved from the character-based lending to ideology-based lending to today competitiveness-based lending in the context of India's economic liberalization policies and the process of

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

linking with the global economy (Singh, 2005). The banking sector of India accommodates 1,175,149 employees, with total of 1, 09, 811 branches in India (and 171 branches abroad), and manages an aggregate deposit of Rs. 67,504.54 billion (US$1.1 trillion) and bank credit of Rs. 52,604.59 billion (US$870 billion). The net profit of the banks operating in India was Rs. 1,027.51 billion (US$17 billion) against a turnover of Rs. 9,148.59 billion (US$150 billion) for the financial year 2012-13. The public-sector banks (PSB) accounted for 74.6% of bank deposits while private sector banks had only 18%, with the rest of the funds lying with regional rural banks and foreign banks. Interestingly, it is the private banks (including foreign banks), which stand for perfection and are well-known for their prompt services that appear to be more prone to banking frauds. The private sector banks, however, have implemented the state-of-the-art systems and have been among the front-runners in investing in new technology. The phenomenal spread of branches, growth and diversification in business, large-scale computerization and networking, have collectively increased manifold the operational risks faced by banks (Bhasin, 2007). In fact, globalization and deregulation have opened up new frontiers for banks to augment their revenues. The pressure to grow rapidly in a highly competitive environment has also given a new dimension to managing operations risk—the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. Reserve Bank of India (RBI) is the regulatory body, keeping an eye, over banking industry.

It is inevitable that such a huge Indian banking industry is also prone to many frauds. The KPMG "India Fraud Survey 2012" states "Despite having a strong regulator, the financial services sector has emerged as the most susceptible sector to fraud. The misuse of technology in the banking sector includes use of banking access for over-payments to vendors or self-bank account, sharing of potential confidential information and misuse of the company's technology resources for unauthorized activities, which includes conflicting business relationship. Also, providing services on mobile and social media platforms with limited knowledge of the security requirements, poses lot of threats to customers as well as the financial institutions." Given the weaknesses in Indian law enforcement regarding the investigation and prosecution of fraudsters and the ever increasing social pressure to get rich quickly, fraud remains a constant danger to businesses. "The confidence of international investors and domestic entrepreneurs has been low in the last two years, thanks to the various scams that have come to light during this period."

Recently, banking sector business has become more complex with the development in the field of information and communication technology (ICT), which has changed the nature of bank fraud and fraudulent practices. For example, Berney (2008) observes that customers rely heavily on the web for their banking business, which leads to an increase in the number of online transactions. Similarly, Gates and Jacob (2009), and Malphrus (2009) have asserted that "the internet provides fraudsters with more opportunities to attack customers, who are not physically present on the web to authenticate transactions." Fraud, however, is a major component of operational risk. But if the banker is upright and knows his job well, the task of the defrauder will become extremely difficult, if not impossible. This has thrust enormous responsibilities in terms of prescribing and maintaining an effective architecture of internal checks and controls, and optimum use of innovative technology (Wells 2005).

What is a Fraud?

Fraud is a worldwide phenomenon that affects all continents and all sectors of the economy. Fraud encompasses a wide-range of illicit practices and illegal acts involving intentional deception or misrepresentation. The Institute of Internal Auditors' "International Professional Practices Framework (IPPF)" (2009) defines fraud as: "Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage." Fraud impacts organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. In fact, the losses to reputation, goodwill, and customer relations can be devastating (ACL). As fraud can be perpetrated by any employee within an organization or by those from the outside, therefore, it is important to have an effective fraud management program in place to safeguard your organization's assets and reputation.

One of the most challenging aspects in the Indian banking sector is to make banking transactions free from electronic crime (Pasricha and Mehrotra, 2014). Fraud detection in banking is a critical activity that can span a series of fraud schemes and fraudulent activity from bank employees and customers alike (Sharma, 2003). It may be noted at the outset that all the major operational areas in banking industry offers a good opportunity for fraudsters, with growing fraud and financial malpractices being reported under deposit, loan, and inter-branch accounting transactions (including remittances). Frauds generally take place in a financial system when safeguards and procedural controls are inadequate, or when they are not scrupulously adhered to, thus, leaving the system vulnerable to the perpetrators (Bhasin, 2012). Most of the time, it is difficult to detect frauds well-in-time, and even more difficult to book the offenders because of intricate and lengthy legal requirements and processes. In the fear of damaging the banks reputation, these kinds of incidence are often not brought to light (Ramachandran, 2001). Historical evidence shows that whether the agency (or individual) committing the fraud works for the bank or deals with it, the culprit usually does very careful and detailed planning before he finally attacks the system at its most vulnerable point.

Who is Responsible for Fraud Detection?

While the senior management and the board of Directors of the Banks are ultimately responsible for a fraud management program, internal audit can be a key player in helping to address fraud. By providing an evaluation on the potential for the occurrence of fraud, internal audit can show an organization how it is prepared for and is managing these fraud risks. Instead of relying on reactive measures like whistleblowers, organizations can and should take a more hands-on approach to fraud detection (ACL). A fraud detection and prevention program should include a range of approaches–from point-in-time to recurring and, ultimately, continually for those areas where the risk of fraud warrants. Based on key risk indicators, point-in-time (or ad hoc) testing will help identify transactions to be investigated. If that testing reveals indicators of fraud, recurring testing or continuous analysis should be considered.

In today's automated world, many business processes depend on the use of technology. This allows for people committing fraud to exploit weaknesses in security, controls or oversight in business applications to perpetrate their crimes. However, the good news is that technology can also be a means of combating fraud. Internal audit needs to view technology as a necessary part of their toolkit that can help to prevent and detect fraud (Thomas and Juan, 2001). Leveraging technology to implement continuous fraud prevention programs helps to safeguard organizations from the risk of fraud and reduce the time it takes to uncover fraudulent activity. This helps both to catch fraud faster and to minimize the impact it can have on organizations.

A KPMG (2006) "Forensics Fraud Risk Management" report states, "unlike retrospective analyses, continuous transaction monitoring allows an organization to identify potentially fraudulent transactions on, for example, a daily, weekly, or monthly basis. Organizations frequently use continuous monitoring efforts to focus on narrow bands of transactions, or areas that pose particularly strong risks." By leveraging the power of data analysis technology organizations can detect fraud sooner and reduce the negative impact of significant losses owing to fraud. According to DSCI-KPMG Survey (2010) measures such as SMS alert, separate transaction password, virtual keyboard seem to be more popular, adoption of the strongly advocated measures, such as one-time-password (dynamic token), identity grid and risk-based authentication are still at a nascent stage.

Magnitude of Frauds in Banks: The Indian Banking Industry Scenario

Frauds bleed businesses to the tune of hundreds of billions of dollars worldwide, annually. Innumerable instances of scams and frauds in the global Banking industry have plagued our society since before the Industrial Revolution. According to the Ernst & Young (E&Y) 'India Fraud Indicator 2012,' "Different types of frauds have caused Rs. 6,600 crore loss to the Indian economy in 2011-12, and banks were the most common victims in swindling cases; insider enabled fraud accounted for 61% of the reported fraud cases, and 79% of the major fraud cases were due to involvement of senior management owing to their authority and direct interference in the company's decisions." Rapidly increasing magnitude of bank frauds adversely impacts the Indian economy and makes investors vary about doing business in India. According to Zee Research Group (2013), analysis during the last decade, the Indian banking sector grew at an average rate of 18% in comparison to 7% GDP growth rate. However, during the same period, cyber fraud in the banking sector has emerged as a big problem and a cause of worry for this sector (Soni and Soni, 2013). In a survey conducted by Deloitte (2012), titled "India Banking Fraud Survey – 2012", shows that banks have witnessed a rise in the number of fraud incidents in the last one year, and the trend is likely to continue in the near future. Continued prevalence of this malpractice on a large scale can have disastrous long-term consequences not only for the businesses involved but also for the investors, financial institutions, government, and the economy in general. The central government, therefore, has expressed serious concern over the sharp rise in cases of fraud and corruption especially in the Indian banking industry.

Frauds in the Indian banking industry have seen a steady rise. The country's public-sector banks (PSBs) have reported frauds amounting to nearly Rs. 9,000 crore to the Reserve Bank of India (RBI). And this only in the last three years! This revelation has come after questions were raised in the Lok Sabha regarding the quantum of scams in public sector banks. The numbers throw up a disturbing trend. The RBI, in its report, has reported a rise in number of such cases as follows: "The number of fraud cases reported to RBI by the nationalized banks during the last eight years showing overall a very sharp increasing trend from 1858 cases in 2000-01 to 2658 cases in 2005-06, which declined to 1385 cases in 2007-08" (See **Table 1**). However, the amount involved in fraud cases also increased very sharply from the lowest level of Rs. 374.97 crore during 2002-03 to the highest level of Rs. 1134.39 crore during 2005-06, but the same has declined to Rs.396.86 crore during 2007-08. RBI has further reported that increase in the number of fraud cases during the years 2003-04 (2193 cases) and 2004-05 (2520 cases), as compared to the cases reported during the years 2001-02 (1353 cases), was mainly due to the increase in fraud cases in the area of credit cards, and to some extent, in the housing loans/personal segment. The total number of credit card fraud cases and amount involved during the years 2007-08, 2008-09 and 2009-10 were 17447, 17114 and 18925 cases, and Rs.41.1, Rs. 47.43, and Rs. 54.67 crore, respectively.

Banks these days are being duped of crores of Rupees, thus, destabilizing investor's confidence. For instance, the year 2005-06 witnessed the highest ever wiping of Rs. 1134.39 crore from the banking industry in India due to bank frauds, which was about 2.5 times the amount lost in the previous year. It may be noted here that while the number of fraud cases has shown a decreasing trend from 24,791 cases in 2009-10 to 13,293 cases in 2012-13 (i.e. a decline of 46.37%), the amount involved has increased substantially from Rs. 2037.81 to 8646 crore (i.e. an increase of 324.27%). As on March 31, 2013, commercial banks reported total fraud of Rs. 169,190 crore from 29,910 cases. In 2012-13, Rs. 13,293 crore of fraud was detected in all PSU banks in the country. Further, a bank group-wise analysis of fraud reveals that while the private sector and foreign bank groups accounted for a majority of frauds by number (82.5%), the public sector banks accounted for nearly 83% of total amount involved in all reported frauds. According to Mohul Ghosh (2015), "Between April to December 2014, public sector banks in India incurred losses to the tune of Rs. 11,022 crore due to 2100 cases of fraud, which were higher than Rs.one lakh. Out of the total frauds, Punjab National Bank (PNB) reported maximum amount: Rs. 2306 crore with 123 cases of fraud. On the other hand, State Bank of India (SBI) reported maximum number of fraud cases at 474 but the amount of fraud is low at Rs. 1327 crore. In fact, total frauds discovered between this 9 month period has already surpassed the total frauds reported during 2013-14 fiscal year, when 2593 cases of fraud resulted in loss of Rs. 7542 crore. Thus between the April to Dec.2014, 46% more amount was lost due to frauds compared to last full year."

No doubt, banks are dealing with public's money and hence, it is imperative that employees should exercise due care and diligence in handling the transactions in banks. Our analysis has revealed that "fixing staff accountability is a neglected area so far as public-sector banks are concerned. The general trend is to include a large number of officials in the probe so that the investigation is both delayed and diluted" (Chakrabarty, 2013). It is a matter of concern that the audit systems prevalent in banks have not proved effective in detecting fraud cases due to factors like inadequacy of time allotted for audit, inefficient sampling of transactions to be checked during audit, lack of trained personnel with the required aptitude for audit work, etc. Recent rise in bank fraud calls for tightening of security mechanism. A strong system of internal control is the most effective way of fraud prevention. The banks should increase their efforts to raise the level of security awareness in their organizations to combat frauds.

Table 1: Number of Frauds and Amount Involved in Indian Banks

Year ending 31st March	Amount Involved (Rs. in Crore)	Number of Fraud Cases Reported to RBI
2000-01	538.56	1,858
2001-02	470.37	1,353
2002-03	374.97	1,643
2003-04	823.61	2,193
2004-05	451.04	2,520
2005-06	1134.39	2,658
2006-07	844.76	2,568
2007-08	396.86	1,385
2008-09	1911.68	23,941
2009-10	2037.81	24,791
2010-11	3832.08	19,827
2011-12	4491.54	14,735
2012-13	8646.00	13,293
2013-14	169190.00	29,910

(Source: Compiled by the author from various published bank reports)

Australian Journal of Business and Management Research
New South Wales Research Centre Australia *(NSWRCA)*

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

The PSBs have a 75% market share, but the number of banking frauds by private banks is five times that of PSBs (DNA, 2012). Information obtained under the Right to Information (RTI) Act from the RBI, revealed that while private banks (including foreign banks) have reported about 15,000 cases during 2010-11, PSBs (comprising 19 nationalized banks, including the State Bank of India and its six associates) recorded 3,700 cases. While PSBs lost approximately Rs. 2,500 crore, their better equipped counterparts in the private sector lost Rs. 1,100 crore. The country's largest PSU, State Bank of India tops the charts with frauds to the tune of Rs. 1,221 crore. Bank of India has reported frauds amounting to Rs. 709 crore, Canara Bank has revealed scams worth Rs. 605 crore, IDBI Bank has indicated to RBI on frauds to the tune of Rs. 609 crore. Central Bank has reported frauds amounting to Rs. 562 crore. And this is not it; the entire list submitted in the Lok Sabha indicates that in the last three years, the amount involved in these frauds is a whopping Rs. 8,848 crore and the cases registered are nearly 11,313. Thus, the country's PSBs have reported frauds amounting to nearly Rs. 9,000 crore to the RBI. During 2010-11, the ICICI and HSBC banks put together have reported 13,067 cases. SBI tops the list of PSBs with the highest number of fraud cases reported in the current financial year. SBI reported 784 cases involving Rs298 crore for the year 2010-11, the RTI query revealed. ICICI Bank alone accounted for almost half of the frauds reported to the RBI. Of the 5,319 cases reported in the current financial year (till September) by 29 private banks, a whopping 3,304 were from ICICI. Similarly, in 2010-11, ICICI reported 10,684 of the total 19,845 cases. The second highest numbers of cases were reported by HSBC at 2,383 for the same period. As on March 31, 2013 "Public Sector banks reported 29,653 cases of frauds involving a total amount of Rs. 24,828 crore (83%). While the private sector and foreign bank groups accounted for a majority of frauds by number (82.5%), the PSB accounted for nearly 83% of total amount involved in all reported frauds. "

With the advent of mobile and internet banking, the number of banking frauds in the country is on the rise as banks are losing money to the tune of approximately Rs. 2,500 crore every year. While the figure for 2010-11 was Rs. 3,500 crore, for the current financial year (till September) it is about Rs. 1,800 crore. Further, state-wise list of information on banking frauds shows Maharashtra (Mumbai) reporting the highest number of cases to the RBI. In the last financial year, banks in the Maharashtra reported 1,179 cases with Rs. 1,141 crore being lost to such frauds. Maharashtra is followed by Uttar Pradesh with 385 cases during the same period (Shukla, 2012).

Mumbai is number one for banking fraud in country

Mumbai, as part of Maharashtra State, tops the list of cities with the highest number of frauds reported by banks, with the money involved totaling Rs. 400 crore per year for the past five years. While for the financial year 2010-11, banks in Mumbai reported 787 fraud cases involving Rs. 1,049 crore, the tally for the national capital was 338 cases, with the net amount lost being Rs. 268 crore, as shown in **Table 2**, according to the documents obtained under the Right to Information (RTI) Act from the RBI.

Table 2: Top-ranking State and Incidents of Frauds in Banks in India (2007-08 to 2010-11) (Rs. in crore**)**

Year	**2007**	**2008**	**2008**	**2009**	**2009**	**2010**	**2010 ***	**2011***
States/UTs	**No. of frauds**	**Amount**	**No. of frauds**	**Amount**	**No. of frauds**	**Amount**	**No. of frauds**	**Amount**
Andhra Pradesh	244	83.19	213	93.46	205	73.98	200	148.73
Bihar	51	11.46	69	26.08	55	8.25	71	12.48
Delhi	320	57	365	210.92	349	205.52	338	267.8
Gujarat	125	23.71	229	111.25	115	142.49	122	325.01
Haryana	64	8.31	223	19.72	145	13.84	153	478.59
Karnataka	330	107.12	355	108.26	286	459.21	212	59.61
Madhya Pradesh	121	34.16	130	31.74	97	23.73	288	132.11
Maharashtra	855	203.96	1167	503.14	1006	140.75	1045	682.5
Punjab	105	18.49	135	20.81	104	64.81	173	43.87
Rajasthan	68	38.47	99	76.57	91	9.01	104	19.74
Tamil Nadu	347	144.54	342	166.67	277	175.47	265	81.87
U.P.	331	50.1	344	58.34	281	92.46	329	60.65
West Bengal	308	137.93	348	254.36	242	87.76	317	234.72
Grand Total	**3561**	**1049**	**4432**	**1874**	**3568**	**1669.83**	**3958**	**2681.23**

(Note: The above data relates to only those cases where the amount involved in each case is Rs. one lakh and above. * as on 20-02-2011)

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

Interestingly, the total number of banking frauds reported in Mumbai every year is more than those of Delhi, Chennai, Kolkata and Bangalore taken together. While a five year average figure for Mumbai is about 800 cases, the number for other cities is approximately 200. As per the report, of the 4,099 cases registered in Mumbai since 2006, only 564 cases (those where the amount involved is above Rs. one lakh) have been closed. The city lost Rs. 1,530.35 crore over these five years, of which only Rs. 63 crore has been recovered, reveals the RTI response. Experts blame the low recovery rate on the lack of know-how in detecting and preventing frauds in the era of internet and mobile banking. The banks do not even seem to have the required classification of internet-related frauds. According to the RBI, "there is no distinct category of 'Phishing Complaints'', and as such no separate data/information is classified/compiled in this regard." But phishing is a common method of online identity theft where information such as usernames, password and other bank details are acquired. According to the internet banking guidelines issued by the RBI in 2001, banks need to assess the risks arising out of phishing, consider them as 'operational risk' and cover it with insurance. In this context, Wilson (2006) observes: "Either they are ignoring the RBI mandate or are hiding the information."

In 2004, 127 employees were convicted and 1590 were awarded with major/minor punishment for their fraud offences, which sharply declined by 50% to just 66 employees convicted and 732 awarded penalties. As against this, the number of employees against whom prosecution or departmental proceedings are pending is 1429 in 2004, which marginally declined to 1235 employees. This clearly shows the pathetic, cumbersome and time consuming process of law. It is widely accepted that "action delayed ultimately leads to denial of justice." Moreover, apart from the registered cases, where the recovery rate has been pathetic, many fraud cases are not even registered. Several bankers told DNA that most internet banking frauds cases at the customer level itself, as banks bully the customers into believing that they themselves are responsible.

RBI guidelines for fraud cases

Banking risk management systems are complex, utilizing various tools employing varying levels of integration. Fraud management platforms can include behavioral monitoring, risk profiling, credit-analysis and device reputation to achieve a comprehensive defense in-depth approach. Fraud prevention services must provide a unified approach across all lines of business including retail, card and commercial, while simultaneously preserving the customer experience and improving profitability. As it relates to the online channel, financial institutions need customer-friendly technology that provides protection for their online portals at login, as well as account and transaction creation associated with the entire suite of products and services that they offer.

The RBI requires banks to pursue fraud cases vigorously with the CBI or police authorities, and in court. In the case of PSBs, all fraud cases below Rs. one crore should be reported to the local police, except when the CVO and CMD consider it serious, and when the cases cannot be classified in monetary terms. In those cases, the frauds are referred to the CBI. Cases above Rs. one crore must be referred to a different wing of the CBI depending on the category it falls into. In the case of private-sector banks, frauds of Rs. one lakh and above committed by an outsider, in connivance with a bank official should be referred to the local police. DNA (2012) found that in many of the cases the banks do not follow the RBI guidelines.

The central bank has taken several steps to sensitize banks and curb frauds in the banking industry. So, after RBI learns of the fraud, they examine the case and advise the concerned bank to report the case to the CBI/police or SFIO. Also, it takes measures to recover the amount involved in the fraud. The RBI has also issued several notifications sensitizing banks about common fraud prone areas. It has also issued caution notices against repeat offenders. The evolving fraud landscape around banking and the increase in fraud-related losses requires automated detection systems and robust fraud defense processes (E&Y, 2010).

Review of Literature

Jeffords (1992) examined 910 cases submitted to the "Internal Auditor" during the nine-year period from 1981-1989 to assess the specific risk factors cited in the Treadway Commission Report. Approximately 63 percent of the 910 cases are classified under the internal control risks. Similarly, Calderon and Green (1994) made an analysis of 114 actual cases of corporate fraud published in the "Internal Auditor" from 1986 to 1990. They found that limited separation of duties, false documentation, and inadequate or nonexistent control account for 60 percent of the fraud cases. Moreover, the study found that professional and managerial employees were involved in 45 percent of the cases.

Willson (2006) examined the causes that led to the breakdown of 'Barring' Bank, in his case study, "the collapse of Barring Banks". The collapse resulted due to the failures in management, financial and operational controls of Baring Banks. However, Bhasin (2007) examined the reasons for check frauds, the magnitude of

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

frauds in Indian banks, and the manner in which the expertise of internal auditors can be integrated in order to detect and prevent frauds in banks. In addition to considering the common types of fraud signals, auditors can take several 'proactive' steps to combat frauds. One important challenge for banks, therefore, is the examination of new technology applications for control and security issues.

As per the survey conducted by Ganesh and Raghurama (2008), about 80 executive from Corporation Bank and Karnataka Bank Ltd of India, were requested to rate their subordinates in terms of development of their skills before and after they underwent certain commonly delivered training programs. Responses revealed that for the 17 skills identified, there was improvement in the skills statistically. The paired t-test was applied individually for the seventeen skills, and all these skills have shown statistical significance.

Chiezy and Onu (2013) evaluated the impact of fraud and fraudulent practices on the performance of 24 banks in Nigeria during 2001-2011. Secondary sources of data were used for the study. The relationship between fraud cases and other variables were estimated using Pearson product moment correlation and multiple regression analysis was used. The paper recommended that banks in Nigeria need to strengthen their internal control systems and the regulatory bodies should improve their supervisory role.

The foregoing discussion suggests that the literature on the bank frauds in Indian-context is very limited and inconclusive. Thus, our study builds on the previous literature of bank frauds in the Indian banking sector. The scope of the study has been confined to 21 banks in the National Capital Region (NCR) of India during 2012-13.

Research Methodology

As part of the study, in 2012-13 a questionnaire-based survey was conducted among 345 bank employees of the National Capital Region (NCR) area. It comprised of several questions that attempted to know their opinions while working in a bank regarding training received, attitude towards the procedures prescribed by RBI, awareness level towards frauds and their compliance level under the following six heads: deposit account, loans and advances, administration of passbook and check book, drafts section, internal and inter-branch accounts, and credit-card section.

All the respondents were selected through the random sampling method. There were 42 public sector banks in the area and finally, 21 banks were selected. The sampled employees comprising of Managers, Officers and Clerks of the branches were given the questionnaire by personally visiting them in bank. Out of all the employees, 296 employees responded, with an overall response rate of 85%. In all, there were 57 managers, 130 officers and 109 clerks as respondents and grouped on the basis of the following parameters, as shown in **Table 3**.

Table 3: Classification of Respondents into Categories based on Parameters

Parameter	**Category/Group**		
Compliance score of bank employee	High	Medium	Low
Attitude of bank employee towards procedures prescribed by RBI	Favorable	Moderate	Unfavorable
Training status	Trained	Untrained	
Awareness level of bank employees	High	Medium	Low
Hierarchical level	Managers	Officers	Clerks

Discussion and Analysis of Findings

The RBI has developed many important guidelines for prevention of bank frauds, which can help banks to prevent frauds. The compliance level of these security controls were measured under the following six heads—internal checks, deposit accounts, administration of check books and passbooks, loans and advances, drafts, internal accounts and inter branch accounts. The results of this study indicate that the security control measures are not fully complied with. As per a study, limited separation of duties, false documentation, and inadequate or nonexistent control account for 60% of the fraud cases. It found that professional and managerial employees were involved in 45% of the cases. Thus, education, training and awareness programs are informal intervention measures that should be implemented to prevent frauds. Undoubtedly, security controls prescribed by RBI, if followed with 100% adherence, can prevent frauds to a maximum extent.

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

Table 4: Average Compliance Scores of Various Heads of Bank Managers

	Internal checks	**Loans & advances**	**Deposit account**	**Admin. in check, pass book**	**Draft section**	**Internal & inter-branch account**
Compliance score	95%	91%	82%	65%	84%	83%

Table 4 depicts the average compliance score of Bank Managers under the various heads. The results show that Bank Managers compliance level is the lowest (65%) in administration of check/pass book. In sharp contrast, the highest (95%) compliance is noticed in internal checks. The Managers gave second highest (91%) importance to loans and advances, and gave almost equal importance to the draft section (84%), internal and inter-branch account (83%), and deposit account (82%), respectively. But surprisingly, still there is lack of 100% compliance related to security controls under any of the above listed six bank heads. Thus, it is amply clear that till now, banks in India are not able to follow "zero-tolerance" policy.

Table 5: Average Compliance Scores of Various Heads of Bank Officers

	Loans and advances	**Deposit account**	**Admin. in check, pass book**	**Draft section**	**Internal & inter-branch account**
Compliance score	65%	75%	60%	81%	86%

Table 5 provides a snapshot of average compliance scores of Bank Officers under the various heads. The compliance level of Officers is the "highest" in internal & inter-branch account (86%), followed by draft section (81%) and deposit account (75%). Surprisingly, Bank Officers gave the lowest scores to the following two areas viz., loans and advances (65%), and administration in check and pass book (60%) sections. Keeping in view the Bank Managers and Officers scores, we can draw a broad conclusion: nobody likes to perform the work especially in the administration of check and pass book section." Thus, there appears to be considerable differences in compliance level of employees of various banks, most probably, on account of differences in the organizational culture, training provided, past experiences and their mental attitudes to strictly follow the RBI procedures.

We feel that if the detailed procedures and/or instructions as prescribed by the RBI, if fully complied with (both in letter and spirit), no doubt, it can greatly reduce the incidences of frauds. But the present study revealed "very low percentage of respondents display highly-favorable attitude towards the procedures laid-down by RBI." As **Table 6** shows, a "very high proportion of respondent (98+113=211/296) believe that they do not have sufficient staff to carry out the work meticulously, they are usually overburdened with work and hence, not able to follow the procedures strictly. Since this attitude is based on the perception of bank employees towards adequacy of staff, it can be inferred that "if there is an adequate number of bank staff hopefully the compliance level will be more."

Table 6: Frequency Distribution of the Responses of Bank Employees on the basis of their Attitude towards RBI Procedures

Attitude towards RBI procedures	**Favorable**	**Moderate**	**Unfavorable**	**Total**
Total number of employees	**85**	**98**	**113**	**296**

From **Table 7,** we can conclude that "the compliance level of the managers (48%) is higher than that of officers (22%). This may be due to the fact that managers are more rigorously trained and their attitude towards RBI's procedures is more favorable than that of officers and clerks. Hence, Mangers awareness level is high as they have increased level of responsibility.

Table 7: Distribution of Managers and Officers according to their Compliance Level

Position	**High**	**Medium**	**Low**
Manager	48	42	10
Officer	22	53	25

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

It is amply clear from **Table 8,** the awareness level is very low, both on the part of Clerks and Officers in Banks. For example, only 9.17% of clerks and 13.07% of officers belong to "high" category of awareness level. However, Managers show a little better awareness level. For example, around 15.78% of Managers belong to high category of awareness level. A careful study of the data contained in the table reveals shockingly that about 52% of Clerks, 49% of Officers, and 47% of Managers belong to "low" category of awareness level. It is very disappointing to know that the awareness level of Bank employees about various types of frauds and losses suffered by the banks are very low. Hence, with this dismal scenario, how can we expect from them to follow detailed procedures and guidelines issued by the RBI and take pro-active actions to prevent frauds and mitigate bank losses?

Table 8: Frequency Distribution of the Responses on the basis of Awareness Levels

Awareness Category	**High**		**Medium**		**Low**		**Total**
Position	**Frequency**	**%**	**Frequency**	**%**	**Frequency**	**%**	
Managers	9	15.78	21	36.84	27	47.36	57
Officers	17	13.07	49	37.69	64	49.30	130
Clerks	10	9.17	42	38.53	57	52.29	109

Table 9 depicts the relative importance (on 10 point score) assigned by the Bank Managers, Officers and Clerks to the reasons responsible for the commitment of bank frauds. Managers gave more weight-age to lack of training (7), and followed by overburdened staff (5). In sharp contrast to this, both Officers (6) and Clerks (7) felt that overburdened staff is the main reason responsible for bank frauds, which is followed by lack of training for Officers (5) and Clerks (6), respectively.

Table 9: Score given by Bank Employees to the Various Reasons for Perpetration of Fraud

Position	**Lack of training**	**Corrupt officer in-charge**	**Overburdened staff**	**Competition**
Managers	7	3	5	4
Officers	5	5	6	5
Clerks	6	4	7	4

Discussion on frauds cannot be complete without analysis of human behavior. An employee in a bank is like a fish in a small ocean. Nobody can determine when and how much water a fish has consumed. Likewise a corrupt and dishonest person in a bank can commit frauds with impunity (ACFE, 1996). The total number of bank employees in India against whom the action has been taken for their involvement in cases of bank fraud during 2002, 2003 and 2004 were 5459, 5237 and 4311, respectively. In 2004, 127 employees were convicted and 1590 were awarded with major/minor punishment for their fraud offences, which sharply declined by 50% to just 66 employees convicted and 732 awarded penalties. As against this, the number of employees against whom prosecution or departmental proceedings are pending is 1429 in 2004, which marginally declined to 1235 employees. This clearly shows the pathetic, cumbersome and time consuming process of law. Unfortunately, most of the employees committing frauds get scot free, with the award of minor penalties, and the cases pending in courts keep on dragging for many years. As pointed out by Inamdar (2013), "The time taken for cases to be ascertained as fraud was very high. It took over 10 years for 45% of the cases and between 5 to 10 years for 67% of the cases, creating a great disconnect between the punishment meted out and the offence. But if the delays in bringing fraudsters to book aggravated transgressions, the fact that PSB employees enjoyed a great degree of impunity could have further emboldened those committing the fraud. We observe that in PSBs, most of the officials found liable were let off with minor penalties: caution, warning, censure, stoppage of increments for limited period etc. which sends out a wrong message—a message about passive tolerance rather than active intolerance towards misconduct." It is widely accepted that action delayed ultimately leads to denial of justice.

An analysis of big cases looked into by the CBI reveals that bankers sometimes exceed their discretionary powers, and give loans to unscrupulous borrowers on fake/forged documents. More than 7,000 employees of different PSBs are under the scanner for their involvement in these cases. As B. Venkat Ramana, general manager, corporate communication, UCO Bank said, "The most prevalent nature of cheating and forgery cases relates to forged/fake documents/diversion of funds by borrowers. When fraud is proved with employees' involvement, there is a disciplinary action/criminal case against the employee." According to the General Manager (Risk Management), Bank of Baroda, "the bank immediately carries out an internal investigation if a case of fraud is detected. The incidence is reported to the RBI and a complaint lodged with the local police/state

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

CID/EOW/CBI depending upon the amount involved. In case involvement of the employee is proved, bank takes disciplinary action, which includes even termination/dismissal of the employee."

There is lack of trained and experienced bank staff, and tremendous increase in banking business. By-and-large, new recruits do not have adequate training or experience before they are put into a responsible position. Ganesh and Raghurama (2008) believe that training improves the capabilities of employees by enhancing their skills, knowledge and commitment towards their work. Moreover, bank staff feels "they are overburdened with work." The life has become fast and the bank staff does not have enough time to scrutinize documents thoroughly. Dilution of system and non-adherence to procedures is also a significant reason for bank frauds. This shows that a full-proof system has not been developed and implemented to familiarize the bank employees of various types of frauds that take place in banks every year. "Most banks try to put in place robust systems and controls to prevent fraud and forgery—regrettably crooks and criminals use more and more sophisticated methods, especially where online fraud is concerned, to defraud banks," said Meera Sanyal, former CEO and Chairperson of Royal Bank of Scotland in India (Pai, 2015).

The primary responsibility for preventing frauds lies with individual banks. Major cause for perpetration of fraud is laxity in observance in laid down system and procedures by supervising staff (Sharma and Brahma, 2000). However, the RBI routinely advises banks about major fraud prone areas and the safeguards necessary for prevention of frauds. This is done so that banks can introduce necessary safeguards by way of appropriate procedures and internal checks. With growing usage and dependency on electronic forms of transaction, banks have employed more secured means and platform separate from the normal channels of communication. The authenticity and integrity of such a platform is ensured through usage of specific software, which ensures the validity of the bank's electronic documents (Dubey, 2013). To keep the above frauds at bay, RBI prescribes that bank should conduct annual review of frauds and apprise its board regarding the findings; banks should have proper reporting mechanism in place to report to the RBI all information about frauds and the follow-up action taken. We would like to make the following three recommendations to the banking industry:

- Push top management to implement policies that encourage moral behavior and demonstrate an ethical culture. Appoint a senior person for the anti-fraud group to put fraud prevention and controls on the bank's map;
- Conduct detailed fraud risk assessments to help focus management's attention on the risks to be addressed. These should include specific fraud schemes that could be perpetuated against the bank; and
- Prepare an anti-fraud policy and create appropriate training which clearly defines fraud and misconduct.

CONCLUSION

While the banking industry in India has witnessed a steady growth in its total business and profits, the amount involved in bank frauds has also been on the rise. This unhealthy development in the banking sector produces not only losses to the banks but also affects their credibility adversely (Kaveri, 2014). Recently in April 2015, RBI chief Mr. Rajan has written to the PMO seeking "concerted action in the country's 10 biggest bank frauds allegedly involving prominent real-estate, media and diamond firms that are being probed by the CBI." Accordingly, the government of India has expressed serious concern over the sharp rise in cases of fraud and corruption in the nationalized banks in India. Moreover, fraud and fraudulent activities inflict severe financial difficulties on banks and their customers; they also reduce the amount of money available for the development of the economy (Chiezey and Onu (2013). Many banks and companies that have been victims of frauds are reluctant to share and publicize the facts of the fraud cases due to fear of 'adverse' impact on their reputation (Banks, 2004). Inadequate measure to prevent banking fraud is the primary reason for widespread frauds. So, what should banks do to safeguard the interests of its customers? Banks should ensure that the reporting system is suitably streamlined so that frauds are reported without any delay and fix staff accountability. Banks must provide sufficient focus on the "Fraud Prevention and Management Function" to enable effective investigation of fraud cases. The fraud risk management, fraud monitoring and fraud investigation function must be owned by the bank's CEO, its Audit Committee of the Board and the Special Committee of the Board, at least in respect of large value frauds. Banks can also frame internal policy for fraud risk management and fraud investigation function, based on the governance standards relating to the ownership of the function and accountability for malfunctioning of the fraud risk management process in their banks.

Banks can secure and preserve the safety, integrity and authenticity of the transactions by employing multipoint scrutiny: cryptographic check hurdles. In addition, banks should rotate the services of the persons working on sensitive seats, keep strict vigil of the working, update the technologies employed periodically, and engage more than one person in large-value transactions. Of course, internal auditors can continue to win the battle against frauds and scams through the continued application of fundamentals, such as education, technological proficiency, and support of good management practices. Close attention and vigilance on the part of both banks and customers is, therefore, the best deterrence. According to Freddie Mac (2015), "Fraud Mitigation Best Practices" include: (a) Fraud Risk Management Policies and Procedures: Put sound and appropriate fraud detection, prevention, investigation, resolution, and reporting policies and procedures in place, and communicate them to employees; (b) Regulatory Compliance: Ensure appropriate policies and procedures are in place pertaining to your company's obligations under the RBI Act, as applicable; (c) Ethical Conduct: Familiarize employees with your company's standards for ethical conduct; (d) New Employee Awareness: Incorporate fraud awareness in new employee orientation programs; and (e) Training: Ensure that employees receive fraud training appropriate for their roles and levels.

Banking industry has become more complex with the development in the field of information and communication technology (ICT), which has changed the nature of bank fraud and fraudulent practices. No doubt, technology can prove extremely helpful in perpetuation, detection and prevention of frauds in banks. In relation to banking industry, there is need for greater sharing of information between financial institution on trends and practices of fraudster and fraud topologies, specially those frauds that are committed in computerized environment (McConnell, 2003). Numerous opportunities still exist for dishonest individuals to defraud, and audit practitioners should work with management to consider the 'best' approach to keeping the organization safe from harms. When it comes to fighting fraud and financial crimes, 'proactive' measures yield the best results. As the old adage states, "an ounce of prevention is indeed worth a pound of cure." Recently, data mining techniques are proving extremely helpful to identify unusual patterns in given data set, especially for detecting insider frauds.

As per the documents available, more than 6,000 employees of different banks are under the scanner for involvement in fraud cases. These are not just lower/middle level employees, but in some cases CMDs and directors of different banks. For instance, in May 2013, a CBI special judge convicted Mr. M. Gopalakrishnan, former Chairman-cum-Managing Director of the Indian Bank (Chennai branch) as "he had sanctioned credit facilities of huge amounts to a company without sufficient securities and also by surpassing the rules of the bank." Furthermore, analysis of cases investigated by the CBI reveal that bankers sometimes exceed their discretionary powers and give loans to unscrupulous borrowers on fake/forged documents. After getting the money, the borrower escapes causing huge losses to the banks (Pai and Venkatesh, 2014). There are other reasons too. The increase in alternate channels (including internet banking and even use of ATMs), which have reduced the human interface with the customer and banks has led to an increase in fraudulent activities. "We have already taken corrective measures to ensure preventive vigilance. Policy tightening is also being undertaken," said Mr. M. Narendra, CMD, Indian Overseas Bank. He also added that adequate training is being provided to the staff and the bank is 'fine-tuning operations aspects.' Our analysis has revealed that "fixing staff accountability is a neglected area so far as PSBs are concerned. The general trend is to include a large number of officials in the probe so that the investigation is both delayed and diluted" (Chakrabarty, 2013). Employee training and awareness programs should include fraud awareness in the loan origination and servicing areas.

The wave of financial scandals at the turn of the 21st century elevated the awareness of fraud and the auditor's responsibilities for detecting it (Bhasin, 2013). It is a matter of serious concern that the audit systems prevalent in banks have not proved effective in detecting fraud cases due to factors like inadequacy of time allotted for audit, inefficient sampling of transactions to be checked during audit, lack of trained personnel with the required aptitude for audit work, etc. Internal audit professionals should play an integral role in their organization's fraud-fighting efforts. One important challenge for bank's internal auditors is the examination of 'new' technology applications for control and security issues. The advent of large-scale computerization in banks has opened a new dimension to the concept of fraud and brought about a compelling need for the wholesale review and adoption of a comprehensive fraud prevention control system. According to Thomas and Juan (2001), "The audit environment all over the globe is gradually becoming paperless. Hence, bank internal auditors must adapt to this new environment. Auditors who continue to master the technology used by fraudsters will likely to win the battle." Through proper training, however, internal auditors can curtail the unnecessary exposures facing financial institutions today. The goal, within the banking industry and government, is to create a kind of seamless electronic auditing environment where transactions-related minutiae is routinely scrutinized and the 'exception' process is more easily managed. Both rules and artificial intelligence-based exception-flagging technologies can be effective.

While it is not possible for banks to operate in a 'zero' fraud environment, 'proactive' steps, such as conducting risk assessments of procedures and policies can help them to hedge their risk of contingent losses due to fraud.

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

By leveraging the power of data analysis technology banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud. Moreover, use of new technologies (such as, data visualization, fuzzy logic, social network analysis, data mining, encryption, dynamic account modeling, etc.) can prove handy to mitigate the fraud risk in banks. Although banks cannot be 100% secure against unknown threats, a certain level of preparedness can go a long way in countering fraud risk. At least, it can minimize the damages and protect their reputations.

REFERENCES

1. ACL Services Limted. "Fraud Detection using Data Analytics in the Banking Industry," Discussion paper, available at www.acl.com/bankingfraud, pp.1-8.
2. Association of Certified Fraud Examiners (ACFE), "Report to the Nation on Occupational Fraud and Abuse," The Wells Report, 1996.
3. Banks, David G., "The Fight against Fraud," *Internal Auditor*, April 2004, pp. 34-47.
4. Barnes, R.W., (1995). "The Value of Quality Education to Banks and Bankers," *The Journal of Indian Institute of Bankers*, Vol. 66 no. 3, pp. 55-59.
5. Baruah, S.K. (2015), RBI Chief wants PMO to act against Bank Frauds worth Rs. 17,500 crore, The Hindustan Times, April 24, available at www.hindustantimes.com.
6. Berney, L. (2008) For online merchants, fraud prevention can be a balancing act, *Cards and payments*, Vol. 21, no. 2, pp. 7-22
7. Bhasin, M. L. (2007). The Bank Internal Auditor as Fraud Buster. *The ICFAI Journal of Audit Practice*, Vol. 4, No. 1, January.
8. Bhasin, M. L. (2012), "Corporate Accounting Frauds: A Case Study of Satyam Computers Limited," *International Journal of Contemporary Business Studies*, Vol. 3, No. 10, pp. 16-42.
9. Bhasin, M.L. (2013), An Empirical Investigation of the Relevant Skills of Forensic Accountants: Experience of a Developing Economy, *European Journal of Accounting, Auditing and Finance Research*, Vol. 1, Issue 2, June, pp. 11-52.
10. Chakrabarty, K.C. (2013), "Inaugural Address, National Conference on Financial Fraud," organized by ASSOCHAM, New Delhi, July 26, 2013.
11. Chiezey, U. and Onu, AJ.C. (2013) Impact of fraud and fraudulent practices on the performance of banks in Nigeria, *British Journal of Arts and Social Sciences*, Vol. 15. No. 1.
12. Data Security Council of India (2010), State of Data Security and Privacy in Indian Banking Industry: DSCI-KPMG Survey 2010, published by Data Security Council of India in Feb. 2011.
13. Deloitte Survey, Indian Banking fraud survey-2012, *Business Standard*, February 8, 2012.
14. DNA, Mumbai is number one for banking fraud in country, January 8, 2012
15. DNA, Private banks see more fraud cases than public ones, January 9, 2012
16. Dubey, N. (2013), Banking Frauds: Prevent or Lament, July 11, available at www.mondaq.com.
17. Ernest & Young (2010), Proactive fraud monitoring for banks in India. Available at www.ey.com/india.
18. Ernest & Young (2012), "India Fraud Indicator 2012," a study by Ernst & Young's fraud investigation and dispute services.
19. Freddie Mac (2015), Fraud Mitigation Best Practices, January, available at www.freddiemac.com.
20. Ganesh, A. and Raghurama, A. (2008). Status of training evaluation in commercial bank- a case Study. *Journal of Social Sciences and Management Sciences*, Vol. 37, No.2, Sept, pp 137-58.
21. Gates, T. and Jacob, K. (2009), Payments fraud: perception versus reality, *Economic Perspectives*, Vol. 33 (1), pp. 7-15.
22. Ghosh, Mohul (2015), Rs. 11,022 crore of fraud discovered in public sector banks between April-December 2014, March 23, available at www.trak.in
23. Inamdar, N. (2013), Fraud at public sector banks: a rampant occurrence?, *Business Standard*, November 27, available at www.business-standard.com.
24. Institute of Internal Auditors (2009). International Professional Practices Framework, published by the IIA.
25. Kaveri, V.S. (2014), Bank Frauds in India: Emerging Challenges, *Journal of Commerce and Management Thought*, Vol. 5, no. 1, pp. 14-26.
26. Kumar, V. and Sriganga, B.K. (2014), A review on data mining techniques to detect insider fraud in banks, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, no. 12, December, pp. 370-380.
27. KPMG Survey. *Fraud Risk Management*, 2006.
28. Lok Sabha, Question Hour Reply given by Fianance Minister Mr. P. Chidambaram, "SBI Tops in Bank Frauds," Friday 19 May, 2006 available at Sify.com.

Vol.4 No.12 | April-2015 ISSN: 1839 - 0846

29. Malphrus, S. (2009), Perspectives on retail payments fraud, *Economic Perspectives*, 33(1), pp. 31-6.
30. McConnell, Donald, “Expanded Guidance for Auditor Fraud Detection Responsibilities,” *The CPA Journal*, June 2003, pp.26-33.
31. Pasricha, P. and Mehrotra, S. (2014) Electronic Crime in Indian Banking, *Sai Om Journal of Commerce and Management*, Vol. 1, no. 11, November.
32. Pai, S. Banks no safe havens for your money; depositors lost Rs. 27,000 crore in last five years, DNA, April 8, 2015.
33. Pai, S. and Venkatesh, M. (2014), Frauds ripped public sector banks of Rs. 23,000 crore, *Hindustan Times*, January 30, available at www.hindustantimes.com.
34. Ramachandran, V., “Bank Frauds—Where to Draw the Line,” *The Hindu*, July 23, 2001, available at www.thehindubusinessline.com.
35. Sharma, B.R.(2003). Bank Frauds- Prevention & Detection. Universal law Publishing Co. Ltd.
36. Sharma, S. and Brahma (2000) A Role of Insider in banking Fraud. available at http;/ manuputra .com
37. Shukla, S. PSU banks report frauds worth almost Rs. 8850 crore in last years!, *India Business*, Bloomberg UTV, May 18, 2012.
38. Singh, M.K. (2005) “Bank Frauds—What Every Banker Needs to Know,” *IBA Bulletin*, September, pp. 3-7.
39. Soni, R.R. and Soni, N. (2013), An investigative Study of Banking cyber frauds with special reference to private and public sector banks, *Research journal of Management Sciences*, Vol. 2, no. 7, 22-27 July.
40. Siddharth Tak (2013), Cyber frauds raise their ugly head yet again, *Zee Research Group*. Retrieved from http://zeenews.india.com/exclusive/cyber-frauds-raise-theirugly-head-yet again_6113.html.
41. Thomas, William C. and Alejandro, Juan, “Fraud-Related Audit Issues,” August 2001, *The CPA Journal*, pp.62-64.
42. Wells, Joseph T., “New Approaches to Fraud Deterrence,” *The Chartered Accountant*, May 2005, The Institute of Chartered Accountants of India, New Delhi, pp. 1453-1455.
43. Willson, R. (2006).Understanding the offender/environment dynamics for computer crimes. Information Technology and people Vol, 19, No.2, pp170-186.