British Journal of Research

www.britishjr.org

Original Article

# Combatting Bank Frauds by Integration of Technology: Experience of a Developing Country

**Madan Lal Bhasin***

*School of Accountancy,*
*College of Business, Universiti Utara Malaysia, Sintok, Malaysia*

*Corresponding author e-mail: madan.bhasin@rediffmail.com

**A B S T R A C T**

**Objective:** Fraud is a worldwide phenomenon that affects all continents and all sectors of the economy. With the rapidly growing banking industry in India, frauds are increasing fast, and fraudsters have started using innovative methods.Shockingly, the banking industry in India dubs rising fraud as an inevitable cost of business. One of the most challenging aspects in the Indian banking sector is to make banking transactions free from electronic crime. There is no "one silver bullet" to stop all frauds forever. By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.

**Methods:** The present study is both descriptive and analytical in nature. As part of the study, in 2013-14 a questionnaire-based survey was conducted among 345 bank employees of the National Capital Region area. The questionnaire was structured into two parts. In fact, the first part 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. Moreover, the second part encompassed the issues about how to integrate technology in the banking industry in order to detect and prevent frauds in Indian banks. It also examined the technology solutions available and how to integrate forensic approach to combat bank frauds in the Indian banking industry.

**Results:** The present study indicates there is 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. Bank Managers compliance level is the lowest in administration of check/pass book; while highest compliance is noticed in internal checks. Banks in India are not able to follow "zero-tolerance" policy. There is considerable difference in compliance level of employees of various banks on account of differences in the organizational culture, training provided, past experiences and their mental

attitudes to strictly follow the RBI procedures.
Mostly ffrauds in the banking institutions are detected through customer complaints, followed by an internal or external tip, which is in line with global trends.Although banks cannot be 100% secure against unknown threats, a certain level of preparedness can go a long way in countering fraud risk. Internal audit professionals should play an integral role in their organization's fraud-fighting efforts. Some of other promising steps to control frauds are: educate customers about fraud prevention, make application of laws more stringent, leverage the power of data analysis technologies, follow fraud mitigation best practices, and employ multipoint scrutiny.
**Conclusion:** Promising steps to control frauds are: educate customers about fraud prevention, make application of laws more stringent, leverage the power of data analysis technologies, follow fraud mitigation best practices, and employ multipoint scrutiny. In 2015, the RBI has introduced new mechanisms for banks to check loan frauds by taking pro-active steps by setting up a Central Fraud Registry, introduced the concept of Red Flagged Account, and Indian investigative agencies (CBI, CEIB) will soon start sharing their databases with banks. Although banks cannot be 100% secure against unknown threats, a certain level of preparedness can go a long way in countering fraud risk.

**Keywords:** Bank frauds, banking industry, RBI,risk management, use of technology, current scenario, future challenges.

## INTRODUCTION

It is universally accepted that for the smooth functioning of a money market and economic growth of a country, an efficient and good banking system is a must. Banking industry in India has traversed a long-way to assume its present stature in the21st century. According to Singh,[1]"The Indian banking industry is unique and has no parallels in the banking history of any country in the world. After independence, the banking sector has passed through three stages: character-based lending to ideology-based lending to competitiveness-based lending." Similarly, Kumar and Sriganga[2] stated, "Banking sector of India accommodates 1175,149 employees, with total of 109,811 branches in India (and 171 branches abroad), and manages an aggregate deposit of Rs. 67,504.54 billion and bank credit of Rs. 52,604.59 billion." Indeed, PSBs have a 75% market share, but the number of funds by private banks is 5 times of PSBs. The phenomenal spread of branches, growth and diversification in business, large-scale computerization and networking, have collectively increased manifold the operational risks faced by the banks. Unfortunately, it is also true banking industry has to face many types of frauds and scams. The Reserve Bank of India (RBI) is the central policy making and national-level regulatory body by keeping an eye over the entire banking industry.

Recently, Pan[3] stated that "deposits of Indian banking industry is Rs. 81 trillion (USD1.30 trillion) in 2014. Banks are using internet and mobile devices to carry out transactions and communicate with the masses." Moreover, according to KPMG-CII report[4] "Indian banking sector has potential to become 5th largest in the world by 2020, and 3rd largest by 2025." Besides, Kaveri[5] remarked that "while the Indian banking industry has witnessed a rapid growth in their business and profits, the amount involved in bank frauds has also been on the rise. This unhealthy development causes losses to the banks and badly affects their credibility." As KPMG's 'India Fraud Survey 2012'[6] states, "Despite having a

strong regulator, the financial services sector has emerged as the most susceptible sector to frauds." Fraudulent activities cause losses to banks and their customers, and also reduce money available for the development of economy.[7] Shockingly, "the banking industry in India dubs rising fraud as an inevitable cost of business" (E&Y). According to Deloitte India Banking Fraud Survey Report[8] (Edition II, 2015), "Common causes of frauds in banking include diversion & siphoning of funds, whereas fraudulent documentation and absence, or overvaluation of collaterals were the main reasons for fraud in retail banking." Thus, in nutshell, "inadequate measures to prevent banking fraud is the primary reason for widespread frauds. Technology is like a double-edged sword[9], which can be used to perpetuate, detect and prevent frauds."

However, Gates and Jacob[10] have pointed out that "the misuse of technology in the banking includes use of banking access for over-payments to vendors, sharing confidential information, and misuse of technology for unauthorized activities." Also, providing services on mobile and social media platforms, with limited knowledge of security requirements, poses lot of threats to customers and banks.[11] Data analysis software enables auditors and fraud examiners to analyze an organization's business data to gain insight into how well internal controls are operating and toidentify transactions that indicate fraudulent activity or the heightened risk of fraud[12]. Data analysis can be applied to just about anywhere in an organization where electronic transactions are recorded and stored. As Kumar and Sriganga stated, "By leveraging power of data analysis technology, banks can detect fraud very soon and reduce the impact of losses due to frauds. Use of new technology can prove to be very helpful to control the fraud risk in banks[2]." It is a well-known fact that investigation and prosecution of fraudsters in India is "very slow, time-consuming process, thus, the danger of fraud will always be there. 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.

Recently, banking sector business has become more complex with the development in the field of information and communication technology, which has changed the nature of bank fraud and fraudulent practices. For example, Berney[13] observed 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,[10] and Malphrus[14] 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.[15]Banks have more technology and more incentive than ever to combat fraud in electronic banking services. But whether they have enough technology and incentive to protect consumers from the headaches of a compromised account, payment card or identity is doubtful.

## Meaning and Types of Bank Frauds

Fraud is a worldwide phenomenon that affects all continents and all sectors of the economy. As per RBI, fraud can be "loosely" described as "any behavior by which one person intends to gain a dishonest

advantage over another." 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)"[16] 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 bestaggering. In fact, the losses to reputation, goodwill, and customer relations can be devastating. 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.

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,[17] "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.

One of the most challenging aspects in the Indian banking sector is to make banking transactions free from electronic crime[18]. 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. 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.[19] 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. 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. Table 1 shows some of the common types of frauds in the Indian banking sector.

In today's volatile economic environment, the opportunity and incentive to commit frauds have both increased. Instances of as set misappropriation, money laundering, cyber crime and accounting fraud are only increasing day-by-day. With changes in technology, frauds have taken the shape and modalities of organized crime, deploying increasingly sophisticated and innovative methods of perpetration. In the 21st century, as financial transactions become increasingly technology-driven, new technology seems to have become the weapon of choice, when it comes to fraudsters.

According to the PwC[20] Global Economic Crime Survey 2014, "cybercrime was one of the top economic crimes reported by organizations across the world, including India." Regulations and laws governing the financial services sector in India are continuously evolving. For any growing organization, it is critical to keep up with the changing laws in order to mitigate risks and stay ahead. Some of the important regulatory drivers for the financial sector in India are as follows: (a) Reserve Bank of India Act, 1934; (b) Securities and Exchange Board of India Act, 1992; (c) Companies Act, 2013; (d) Prevention of Money Laundering Act, 2002; and (e) The Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015. The PwC's Survey identified that suspicious transaction reporting, effective fraud risk management measures, whistle blowing processes and tip-offs helped financial services organizations to detect most frauds.

There is no simple way to squash fraud, but by implementing the right mix of technologies and prevention techniques, treasury executives can greatly reduce their organization's risk. As Accenture's Santoro puts it, "A solid portfolio of solutions with multiple layers of protection and controls can go a long way toward providing the necessary protection. If you put enough deadbolts at the door, thieves are going to give up and look elsewhere." It is an endless game of "cat and mouse" between banks and cyber-criminals. There is a virtual arms race taking place online between financial institutions and cyber criminals, who as soon as the bank deploys a new process or technology to prevent online fraud, they find a weakness to exploit.[11,21] In addition, customers expect to be protected from fraud, but also want anti-fraud tools to look at them holistically, assessing the fraud risk of transactions based on their individual profiles. Five ways to combat bank frauds are highlighted below as:

**1.** ***Adopt appropriate technologies:*** An inclusive mix of strong authentication systems; analytics software; and bank services, positive pay and payee verification, for example, can greatly reduce an organization's exposure to fraud. It is important to have layers of protection.

**2.** ***Beef up your internal controls:*** Sarbanes-Oxley mandates that companies pay strict attention to their internal controls. But even the most thorough Sarbanes-Oxley compliance effort cannot provide comprehensive protection against fraud. Proactive organizations will want to put additional controls in place, including rigorous approval procedures and careful separation of duties. That is especially true of disbursement processes, such as wire transfers.

**3.** ***Screen job applicants carefully:*** One of the biggest security problems company's face is fraud perpetrated by trusted insiders. Key finance functions such as treasury must conduct background checks on potential hires, and companies should also consider drug testing and honesty testing. It is the first line of defense.

**4.** ***Educate your workforce:*** Employees need to understand how damaging fraud can be to the organization. They must be able to recognize signs of fraudulent activity and know how to report it. In addition, treasury employees will need to betrained in the correct use of the company's fraud-protection tools and technologies.

**5.** ***Prosecute thieves:*** Many organizations fire employees who are caught stealing but avoid prosecuting them for fear of bad publicity. A zero-tolerance policy goes a long way toward reducing the risk of illegal activity. Likewise, managers should immediately turn over any evidence of suspected fraud to law enforcement agencies.

## 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.[11] 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. According to Deloitte India Banking Fraud Survey Edition II (2015), "Some of the top reasons for increase in fraud incidents are: (a) Lack of oversight by line managers/senior management on deviations from existing processes, (b) Business pressures to meet unreasonable targets, (c) Lack of tools to identify potential red flags, and (d) Collusion between employees and external parties."[8]

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. 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. According to ACL,[11] the analytical techniques, which may prove very effective in detecting fraud, are shown below:

- Calculation of statistical parameters to identify outliers that could indicate fraud
- Classification to find patterns amongst data elements
- Stratification of numbers to identify unusual entries
- Digital analysis using Benford's Law to identify unexpected occurrences of digits in naturally occurring data sets.
- Joining different diverse sources to

identify matching values where they should not exist

- Duplicate testing to identify duplicate transactions such as payments, claims or expense report items.
- Gap testing to identify missing values in sequential data where there should be none.
- Summing of numeric values to identify control totals that may have been falsified
- Validating entry dates to identify suspicious items for postings or data entry.

As very strongly emphasized by Bhasin,[22] "In the 21st century, the forensic accountants are in great demand and forensic accounting is listed among the top-20 careers of the future." Recent accounting scandals and the resultant outcry for transparency and honesty in reporting, therefore, have given rise to two disparate yet logical outcomes. First, forensic accounting skills have become very crucial in untangling the complicated accounting maneuvers' that have obfuscated financial statements. Second, public demand for change and subsequent regulatory action has transformed corporate governance (CG) scenario[23]. Therefore, many senior-level company officers and directors are under the ethical and legal scrutiny. In fact, both these trends have the common goal of addressing the investors' concerns about the transparent financial reporting system. The failure of the corporate communication structure has also made the financial community realize that there is a great need for skilled professionals that can identify, expose, and prevent structural weaknesses in three key areas: poor CG, flawed internal controls, and fraudulent financial statements.[24] Therefore, forensic accounting skills are becoming increasingly relied upon within a corporate reporting system that emphasizes its accountability and responsibility to stakeholders.

## Magnitude of Frauds in Banks: Indian Banking Industry Scenario

Different types of frauds caused Rs. 6,600 crores of 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 fraud cases. However, Soni and Soni[25] concluded that "cyber fraud in the banking industry has emerged as a big problem and a cause of worry for this sector." Similarly, another survey conducted by Deloitte[26] 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." The Deloitte India Banking Fraud Survey Report Edition II added, "the number of frauds in banking sector have increased by more than 10% over the last two years. Banks witnessed rise in level of sophistication with which frauds were executed."[8] It is universally accepted that continued prevalence of frauds will have long-term bad consequences for banks, customers, investors, government and the economy in general.

The year-wise details, beginning from 2000-01 to 2013-14, regarding the number and amount of frauds reported by the Indian banking sector to the RBI, are shown in Table 2. The following broad generalizations can be made. During the last six years, from 2000-01 to 2005-06, the number of fraud cases has shown a constantly rising trend. For example, in 2000-01 there were 1858 cases of frauds, which substantially jumped to 2658 fraud cases in 2005-06. However, in 2006-07 and 2007-08, the number of fraud cases declined sharply from 2568 to 1385, respectively. In fact, the amount involved in fraud cases has 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. The year 2007-08 was an exceptional year in which the amount of loss caused due to fraud declined to Rs. 396.86 crore. In sharp contrast to this, year 2005-06 was also a very significant year for the banking industry, since this year witnessed the highest ever fraud loss of Rs. 1134.39 crore. Keeping in view the loss of Rs. 451.04 crore in 2004-05, the loss of Rs. 1134.39 crore in 2005-06, works out to about 2.5 times the loss of previous year. Moreover, the scenario of number of frauds and amount involved has significantly changed from 2008-09 to 2013-14. For example, 24,791 cases of frauds were reported in 2009-10, which showed a constant trend of decline till 2012-13. Number of fraud cases reported were 19,827 in 2010-11, which declined to 14,735 cases in 2011-12, and 13,293 cases in 2012-13 (a decline of 46.37%), respectively. As against this, the trend has reversed when we have a look at the amount of loss suffered by banks during the same period. For instance, the amount of loss suffered has increased very sharply from Rs. 2037.81 crore in 2009-10 to Rs. 8646 crore in 2012-13, an increase of 324.27%. As Pai and Venkatesh[27] (2014) reported, "As on March 31, 2014 banks reported total loss of Rs. 169,190 crore from 29,910 cases. In 2012-13, Rs. 13,293 crore of fraud was detected from 8646 cases." During Apr.-Dec. 2014, PSBs suffered losses of Rs. 11,022 crore from 2100 fraud cases involving Rs. one lakh or more. During same period, 46% more amount was lost due to frauds compared to last full-year.

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.

## Review of Literature

Jeffords[28] (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[29] 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% of the cases. Ziegenfuss[30] performed a study to determine the amount and type of fraud occurring in state and local government.

Willson[31] 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[32] examined the reasons for check frauds, the magnitude of 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. In another study, Bhasin[33] examined in-depth the corporate accounting fraud perpetuated by the Satyam management team in collusion with the auditor.

As per the survey conducted by Ganesh and Raghurama[34], 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. Moreover, another study to investigate the reasons for bank frauds and implementation of preventive security controls in Indian banking industry was performed by Khanna and Arora[35]. The study "seeks to evaluate the various causes that are responsible for bank frauds. The result indicate that lack of training, overburdened staff, competition, low compliance level are the main reasons for bank frauds."

Mhamane and Lobo[36] in their study attempted to detect and prevent fraud in case of internet banking using Hidden Markov Model algorithm. Chiezy and Onu[7] 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. However, Dzomira[21] investigated the use of digital analytical tools and technologies in electronic fraud and detection used in the Zimbabwe banking industry. He concluded that banking institutions should reshape their anti-fraud strategies to be effective by considering frauds detection efforts using advanced analytics and related tools, software and application to get more efficient oversight. Similarly, Kumar and Sriganga[2] highlighted the common insider frauds occurring in banks and also tried to categorize them into different types. They focused on different generic data mining techniques and in specific, the techniques used for detecting insider frauds.

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.

## Research Methodology

The present study is both descriptive and analytical in nature. As part of the study, in 2013-14 a questionnaire-based survey was conducted among 345 bank employees of the National Capital Region (NCR) area. The questionnaire was structured into two parts.In fact, the first part 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. Moreover, the second part encompassed the issues about how to

integrate technologyin the banking industry in order to detect and prevent frauds in Indian banks. It also examined the technology solutions available and how to integrate forensic approach to combat bank frauds in the Indian banking industry.

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.

## Findings and Analysis of Data

The RBI, being the overall central regulatory agency, has developed many important guidelines for prevention of bank frauds, which can help banks to prevent frauds. In the first part of the questionnaire, we focused on 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.

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.[37]

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 (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."

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.

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 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.

When we asked the bank employees and managers, 80% indicated that fraud detection tools and technologies are the most effective ways of combatting bank frauds. On the other hand, 43% of the respondents showed that real-time decision making tools are effective in preventing fraud, while 22% respondents showed that monitoring of accounts is effective, whilst 77% indicated that customer awareness is most effective of preventing fraud, and finally, 76% of the respondents revealed that training of employee putting emphasis on identification and response to fraudulent activities is the most effective way of preventing fraud in organisations. The response given by Bank Employees and Bank Managers are shown in Table 10.

Based on how fraud incident is typically detected in bank, a large majority of 21% respondents gave the reason of complaint by a customer. However, the second important reasons given by 18% of respondents were internal whistle-blower and during audit of accounts or reconciliation process. Over 16% of respondents gave the reason "through automated data analysis or transaction monitoring software." Moreover, other important reasons given by the respondents were: at the point of transaction (10%), through a third-party notification (7%), by accident (6%) and review by a law enforcement agency (4%), respectively. To

conclude, as shown in Table 11,survey respondents indicated that frauds in their organizations were most commonly detected through customer complaints, followed by an internal or external tip, which is in line with global trends.

Banks response to fraud is critical as it has the ability to prevent future occurrences. Any response to fraud should be swift and effective so as to percolate the right message to employees. According to a 2009 Circular issued by RBIstates, "Banks to investigate frauds of large values with the help of skilled manpower in order to effectively take internal punitive action against the staff in question, along with external legal prosecution of the fraudsters and their abettors, if required." In line with RBI's recommendations, the majority of thesurvey respondents indicated that upon the detectionof fraud, they carried out internal investigations, whileothers reported the incident to a law enforcementagency (see Table 12). The reasons given by respondents were: internal investigation is done (46%), incident reported to legal agency (32%), and forced to resign (14%). It is interesting to note that only 8% ofsurvey respondents indicated using an independentconsultant to carry out investigations. Survey respondents indicated that the top three challenges faced by banks in preventing fraud were: lack of customer awareness (23%); integration of data from various sources (20%); and inadequate fraud detection tools (18%).

It is important to understand that fraud investigation requires specific skill sets like "forensic accounting and technology" to collect adequate evidence, which can be admissible in a court of law.[38] In the absence of these, banks may not have the confidence to take legal resource or action on the fraudster, which could be one of the reasons why banks may not be reporting all the cases to law enforcement agencies. While theresponses received in our survey indicate that banks haveset up a dedicated fraud investigative cell, it appears to be hampered by thelack of dedicated technology tools for investigation. Alittle over 40% of survey respondents indicatedthey had not started implementing dedicated forensic technology tools for investigation, whereas, 20% of respondents had partially implemented these tools.Only 20% indicated that they had implemented forensic technology tools for investigation, and that thesetools were effective.

The second part of the questionnaire focussed very specifically about the use of technology in banks. Accordingly, we asked the Bank Employees and Bank Managers regarding the most effective methodologies used by them in banks to detect and prevent frauds. The response given by Bank Employees and Bank Managers are shown in Table 13.An overwhelming majority of 85% of the respondents indicated that they are planning to use in their bank intrusion prevention technologies. However, 78% of the respondents expressed the opinion that fraud management system be planned for use. However, 68% of the respondents revealed that they intend to use strong encryption techniques in future, and 70% indicated that they plan to apply neural net fraud detection technologies. As against this, 62% of the respondents plan to use strong authentication, as on-going fraud prevention and detection program in future.

According to the responses received, 53% of the respondents appear to have implemented a dedicated fraud detection/analytics solution. However, only one in every three respondents appears to be entirely satisfied with it. The following responses were given by the respondents, in order of response: ability to highlight red-flags where controls are being circumvented (29%),ability to identify where enhanced controls are needed (27%), provide

enhanced tracking of high-risk customers (19%), provide case management abilities (13%) and provide audit trails (12%), respectively (see Table 14). Thus, it was interesting to note that 56% of respondents sought technology to help them either highlight red-flag areas (29%), where controls have been circumvented, or where controls needed to be enhanced (27%). We feel this could be because banks have realized that "deviation from existing controls by line managers/supervisors is one of the major causes of fraud in this sector." With technology available, which can help banks detect these deviations in controls, the internal audit team can also leverage this solution to undertake forensic based audits, which could go a long way in enhancing the efficiency of detecting frauds in time.[39]

Since banks are increasingly depending on technology, it is not surprising to find that cybercrime continues to increase in volume, frequency and sophistication. This includes ATM skimming, phishing/vishing and misuse of credit and debit cards[40] (Bhasin, 2007). Table 15 shows that ATM frauds ranked first with 23%, phishing and vishing attacks with 16%, mortgage with 114%, credit cards with 10%. Others (37%), includes options such as third-party POS skimming, account takeover fraud, IP theft, money laundering etc. Additionally, when asked to select the top three areas which were giving sleepless nights to bankers, it was no wonder that internet banking/ATM fraud, E-Banking and identity fraud were the top culprits. Interestingly, mortgage portfolio also appears to be increasingly vulnerable to the risk of fraud.

Also, we asked the respondents some questions about "the demand for FCAs in the future—next five, ten and twenty years." As can be seen from Table 16, the majority of respondents felt that the demand for FCAs will increase well into the foreseeable future. In fact, ninety-four percent felt that the demand for FCAs would increase in the next 10 years. Respondents were also asked "if they felt that there will be enough FCAs available to meet the demand in the next five, or ten years, and beyond the next 10 years." As can be seen in Table 17, many participants were unsure if the supply of FCAs would be enough to meet the demand in the future.

Recently, the banking industry around the world has undergone a tremendous change in the way business is conducted. As pointed out by Bhasin[41], "Leading banks are using Data Mining (DM) tools for customer segmentation and profitability, credit scoring and approval, predicting payment default, marketing, detecting fraudulent transactions, etc." Finally, the sampled respondents were asked, "In general, do FCAs needs to know computer-based forensic techniques?" Eighty-four percent of the respondents answered in "yes" to this question. Moreover, we asked the respondents "how important four different software tools are for FCAs: ACL, IDEA, Data Mining, and Digital Evidence Recovery**.**" The scales were anchored at each end with the descriptors "extremely unimportant" and "extremely important," respectively. For the purpose of analysis, the descriptor "extremely unimportant" was given a weight of 1, while the descriptor "extremely important" was given a weight of 7. The mid-point of the scale "neither" was given a weight of 4. Table 18shows the results. The respondents rated each of these four tools as important, with data mining being rated as the most important with a mean score of 5.83.

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.[42] 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. 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.[43]

Recently, the RBI[44] pointed out that "detection of fraud takes very long-time, and banks tend to report an account as fraud only when they exhaust the chances of recovery. Delays in reporting of frauds further delay the alerting of other banks about the modus operandi through caution advices that may result in similar frauds being perpetrated elsewhere." Bhasin[45]concluded "In the current environment, forensic accountants are in great demand for their accounting, auditing, legal, and investigative skills in order to detect and prevent frauds and scams in the Indian banking sector." 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. VenkatRamana[46], 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 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.[47]

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. Undoubtedly, training improves the capabilities of employees by enhancing their skills, knowledge and commitment towards their work.[34] 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.[27]

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. 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.[48] 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: (a) 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; (b) 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 (c) Prepare an anti-fraud policy and create appropriate training which clearly defines fraud and misconduct.

## How Technology is Shaping the Fight Against Bank Frauds?

Technology is like a double-edged sword. On the one hand, perpetrators are using it to further fraudulent schemes; on the other hand, we are making some of our best progress using the same technology. Undoubtedly, technology can prove helpful in fraud detection and prevention in banks.[49]Unfortunately, the fraud takes on many forms to be handled with any 'single' application or approach. The cat and mouse game will continue. As technology becomes more advanced, fraudulent schemes will become more complex, while more sophisticated fraud solutions will be developed to combat hackers' best efforts. As the landscape of fraud continues to shift, business leaders must be aware of trends and predictions that will allow them to implement internal/external controls and systems to help reduce the risk of fraud and keep them from becoming another statistic.[50]By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.

Neural Networks have been extensively put to use in the are as of banking, finance and insurance. Usually such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends. Fraud cases are statistically analysed to derive out relationships among input data and values for certainkey parameters in order to understand the various patterns of fraud. This knowledge of fraud trends is then iterativelytaught to feed-forward neural networks, which can successfully identify similar fraud cases occurring in the future.[51]In the realm of fraud detection, the ability to revealrelationships, transactions, locations and patternscan make the difference between uncovering a fraudscheme at an early stage as opposed to having it grow into a major incident. From money-launderingschemes to anti-corruption laws, from manipulatingfinancial statements by reporting fictitious revenues toinappropriate sanctioning; forensic analytical tools canhelp explore data and quickly identify errors, irregularities and suspicious transactions embedded within your business, thereby providing clarity to concerns raised by managers and employees[52].

Whether it is financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the banking sector. Most banks are,

therefore, insisting on cashless and paperless transactions. The substantially larger proportion of technology related frauds in the Indian banking sector by number is only expected as there has been a remarkable shift in the service delivery model with greater technology integration in the banking industry. Even though the incidence of cyber frauds is extremely high, the actual amount involved is generally very low. The new technologies adopted by banks are making them increasingly vulnerable to various risks, such as, phishing, identity theft, cards kimming, vishing (voicemail), SMSishing (text messages), Whaling (targeted phising on high net worth individuals),viruses and Trojans, spyware and adware, social engineering.[53,56] Changing technology and rapid flow of information have placed the customer at the center. It is critical for every bank to understand customer needs and expectations and offer customized services.

While some of the risks in the banking sector have always been there, they keep on changing with the constantly evolving technology standards and regulatory framework. Part of the challenge is that the types of financial fraud and characteristics of fraudsters have changed in recent years. For instance, check fraud is in decline while electronic fraud is on the rise, and the latter tends to be perpetrated by more sophisticated criminals. Cheque fraud has been around the globe since the ancient time, but the pace of changing schemes has been very slow for banks to react with very good procedures—many of them still 'manual'. According to Bhasin[54], "Some of the technological innovations, which may be already in use in some banks are: (a) Two-dimensional Bar Codes, (b) Data Glyphs, (c) Biometrics, (d) Cheque Image Processing, (e) Data Mining (f) Data Analytics, etc." Given this complicated fraud prevention picture, banks will need to figure out their own patterns of exposure and deploy tools with the best fit. Banks have more technology and more incentive than ever to combat fraud in electronic banking services. But whether they have enough technology and incentive to protect consumers from the headaches of a compromised account, payment card or identity is doubtful. Threats are escalating more quickly than what banks, or even just other businesses in general, can deploy in terms of defenses against those threats.[55]

There is no "one silver bullet" to stop all frauds forever. Rather, the pace of new threats is not going to slow down and nobody (no bank, no retailer and no consumer) is ever 100%secured. What is needed instead is a combination of checks from a layered approach that banks will have to adopt and consumers will have to accept if they want to utilize electronic banking services. That suggests consumers should expect to see, and might want to welcome, an ongoing stream of new solutions that banks will employ to stay a step ahead of electronic banking fraudsters. It is most unfortunate that the current system of usernames and passwords, with which consumers are familiar, is basically broken. Consequently, banks also have begun to deploy an array of other technologies, some of which are so exotic and sophisticated they might seem like science fiction[56].Here, is a summary of some of the technology that is on tap**:**

- ***Device fingerprinting*** tracks a series of identifiable hardware and software attributes to recognize a user's (or fraudster's) device.
- ***Behavioral analytics*** monitor navigation techniques and other aspects of a user's online behavior to search for anomalies or suspicious activity.
- ***Malware detection*** searches for potentially fraudulent changes to a user's

Web browser to assess whether it's been compromised.

- ***Knowledge-based authentication*** presents a series of static or dynamic and supposedly secret questions to establish a user's identity.
- ***Password tokens*** give a user a one-time-only password that must be entered before it expires.
- ***Out-of-band authentication*** challenges a user to access a one-time-only password or code that is sent to another device, such as a mobile phone or land line.
- ***Transaction signing*** requires a user to digitally sign each transaction.
- ***Endpoint protection*** requires a user to download a one-time-only, secure browser to access a website.
- ***Voice printing*** records attributes of a caller's speech over time and matches those attributes against subsequent calls. Voice printing is an example of biometrics, which use unique physical traits, or characteristics to identify individuals.

However, as technology advances, we are seeing a distinct proliferation of more complex fraud schemes. At the same time, we are seeing more breakthroughs in the use of technology to detect fraud. Strategies that we have used in just the past few years will become completely outdated, as a fresh set of tactics will debut.[50] To minimize the potential damage of fraud, companies need to invest not just in more advanced technology but in people and policies for detecting attacks as quickly as possible. While the networks are just too large to prevent every attack from occurring, detection is crucial. Most companies do not have adequate protocols and staff in place to deal with incidents of fraud. While advanced technology serves as a great tool to combat fraud, the issue should be viewed as more than just an IT problem and looked at as a business problem. Remember, the cost of trying to prevent fraud is far less expensive to a business than the cost of fraud committed on a business.[51]

## Global Trends in Fraud Prevention and Detection

Technology can play a major part in combatting new age frauds, the E&Y Fraud Survey[57] noted and added that a "proactive Forensic Data Analysis" can help governments, regulatory bodies and corporate to counter the increasingly complex nature of frauds. 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. Some techniques such as data visualization have proved to be effective. Fuzzy logic is another technique, which can be used on the data records of a company. These clubbed with a social network analysis, can indicate possible threat of collusion. Progressive reviews of unstructured data can help banks analyze the sentiments, tones and elements described in the fraud triangle (incentive, pressure and rationalization). This, together with unsupervised pattern recognition, can proactively help them to put in place fraud parameters. A careful study of the latest fraud cases in India suggests: (a) banks the most vulnerable, (b) difficult to detect collusion and (c) need for investors to be vigilant. Banks are enhancing their processes, controls and fraud risk management frameworks to minimize the opportunities for fraud, as well as, reduce the time taken in their detection. Many banks are implementing their fraud control and reporting frameworks to generate information in a way that the level of fraud identified, prevented and actual losses incurred are identified. This approach has enabled the benefits of skilled resources and

automated tools to be quantified more precisely.

Regulators and investigative agencies are also trying to gear up for the changed environment. The Central Bureau of Investigation (CBI) announced that it is developing a "Bank Case Information System (BCIS)" to curb banking frauds. This database contains the names of accused persons, borrowers and public servants compiled from the past records[58]. Moreover, the RBI[59] has released "a new framework to check loan frauds by way of early warning signals for banks and red flagging of accounts where defaulters shall have no access to further banking finance." It also has plans to set up a "Central Fraud Registry" that can be accessed by all Indian banks. In addition, the CBI and Central Economic Intelligence Bureau (CEIB) will share their databases with banks. The SEBI is in the process of getting its existing business intelligence gathering software, which is used for detecting fraudulent activities in capital markets, upgraded. Whilst the legal environment and regulators have pushed the financial sector in the right direction, individual institutions are also taking the lead in protecting their earnings and reputation. Some of the top trends include:

- ***Automated Analysis Tools*:** Today, the industry is increasingly aware of the need for automated analysis tools that identify and report fraud attempts in a timely manner. Solution providers are providing real-time transaction screening, third-party screening as well as compliance solutions.
- ***Sector-Oriented Benchmarking Solutions*:** Solutions aimed at assessing the fraud vulnerability of financial institutions are now available. They help in formulating a targeted and cost-effective action plan against fraud risks.
- ***Data Visualization Tools*:** These are being used to provide a visual representation of complex data patterns and outliers to translate multidimensional data into meaningful pictures or graphics.
- ***Behavioral Analytics*:** This is helping businesses identify enemies disguised as customers. The data analytics implemented by the institutions to understand customer behavior, preferences, etc. are also helping in the detection of fraudulent activity either in real-time or post mortem.
- ***Deep Learning*:** Internet payment companies providing alternatives to traditional money transfer methods are using deep learning, a new approach to machine learning and artificial intelligence that is good at identifying complex patterns and characteristics of cybercrime and online fraud.
- ***The Internal Audit Function*:** This function is being altered to include fraud risk management in its scope. The changed technological landscape requires the old ways of internal auditing to give way to new, technologically equipped audit functions. Annual audit planning may no longer be fully effective and flexible audit plans are the need of the hour, as fraud risk assessments require extensive use of forensic and data analytics solutions.

Effective background checks of employees and associates are recommended. It is difficult but also necessary to integrate data from various sources to be able to derive the benefits of analytics techniques. Banks do face challenges in maintaining the efficiency of anti-fraud security controls at an enterprise-wide level. Challenges arise while integrating channels or within applications and tools (integrating online and ATM transactions, retail banking and corporate banking or integrating subsidiary

banks where different information systems are used). The tone at the top is critical in the fight against fraud. Lack of customer and/or staff awareness can result in failure of even the best of technology solutions. It takes a concerted effort to be able to build, maintain and sustain an effective fraud risk management program. Banks need to build awareness around the latest technological and procedural vulnerabilities and fraud schemes, to be able to remain one-step ahead of the fraudsters.

In addition, incident management procedures need to be well-defined and comprehensive, in order to ensure that incidents of fraud are managed without exposing the organization to any legal or reputational risks. Forensic tools can be used to navigate IT systems for evidence of malfeasance such as information deletion, policy violations and unauthorized access. These tools can help the company legal counsels to prepare for a suit to be filed against the fraudster. Apart from internal controls, banks need to also educate the customers. Since the manoeuvres used by cyber-criminals to target sensitive financial data are sophisticated and constantly changing, financial institutions must look at existing security controls with a new approach and risk appetite. The three lines of defense can only be strengthened by technology, not replaced by it.

Customers love online banking for its convenience, while banks benefit from lower costs and a greater reach than a physical branch network provides. Since banking fraudsare going to ultimately affect customer relationship quality and customer loyalty, fraud prevention and its effective communication is very important.[60]In order to ensure that both parties continue to benefit from online banking, it must remain a safe and secure channel that allows legitimate customers access as needed, while simultaneously blocking entrance to cybercriminals. Cybercriminals will continue to target online banking for as long as it is worth their effort to do so. Each instance of online fraud helps additional investment by cybercriminals in the people and technology they need to overcome bank's defenses. Although, there is not a "one-size-fits-all" portfolio of fraud tools and tactics that is applicable to all banks, the following approaches do exist that can prove highly effective in preventing online frauds: (a) multi-factor authentication, (b) geo-location, (c) device recognition, (d) transaction monitoring, (e) navigation controls, (f) cross-channel, and (g) entity-link analysis. Educating the customer on how to help prevent online banking fraud is just one element of a bank's fraud defenses. Deploying advanced technology that can quickly adapt to changes in the cybercriminal's modus operandi is essential to protecting the online channel. Customer must have confidence in the security of a bank's online platform. There is no end in sight, but banks must stay committed to winning each battle they fight to prevent online fraud.[61] To help prevent and detect financial crime, banks need both an integrated (and timely) data set and the ability to bring sophisticated analytics to bear on the data to generate useful insights. Thus, we see the following three major elements for banks that comprise this capability: (a) enhanced data quality, (b) analytics to transform data into information, and information into insight, and (c) application of data visualization techniques.

## 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.[5]

According to Klein[62], "The business firms lose 5% of revenue each year to fraud. When applied to the 2013 estimated gross world product, this revenue loss translates to a global figure of nearly USD3.7 trillion." Accordingly, the Government of India has expressed serious concern over the sharp rise in cases of fraud and corruption in the Indian banking sector. Recently, the 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.[63] 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.[7]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.[64]

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? According to Chakrabarty[65], Deputy Governor of the RBI, "Banks should strengthen their reporting system, quickly report fraud cases, and fix staff accountability. There is urgent need for sharing practices of fraudsters and methods used by such criminals." As Siddique and Rehman[66] stated, "The only promising step is to create awareness among people about their rights and duties, and make application of laws more stringent to check crimes." 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.[67]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.

According to E&Y[57] 'India Fraud Indicator' "Since it is impossible for banks to work in a fraud-free environment, banks should conduct risk assessment of policies and hedge the risk of likely losses due to fraud." Expressing concern over zooming up of the corporate fraud in the last 15 years, Mr. RanjitSinha (CBI Director), said at an ASSOCHAM[68] event, "Rising number of frauds in Indian banks are taking place due to collective failure of regulatory oversight system comprising of external auditors, audit committee, internal audit system, board of directors, independent directors, shareholders, etc. All regulatory and investigative agencies must work in close cooperation and share their inputs and databases with each other in order to prevent frauds." Although banks cannot be 100% secure against unknown threats, a certain level of preparedness can help to face with confidence fraud risks. Recently, the RBI has "established Central Fraud Registry[59] by sharing information about unscrupulous borrowers at the time loans are sanctioned by cross-checking their credentials, and thus, helping banks to control their bad loans. The CBI and Central Economic Intelligence Bureau will also share their databases with banks." The regulators also stressed on prevention of fraud through improved market intelligence. Now, we are hopeful that with the help of new initiatives, banking industry would be able to minimize

the fraud losses, gain customer trust and improve their reputation.

The top three fraud risks that are currently the highest concern to the banks are: (a) Internet banking and ATM fraud, (b) E-banking (credit card and debit card, etc.), and (c) Identity fraud.Despite the proliferation of online and mobile service offerings and the rise in cybercrime, banks and financial institutions can fight back. A comprehensive anti-fraud program can not only protect customers but can cause would-be cyber criminals to turn their attentions elsewhere.

It is important to understand that fraud investigation requires specific skill sets like forensic accounting and technology to collect adequate evidence.[70]While the evidence unearthed by a fraud investigation can vary on a case-to-case basis; typically, it needs to be relevant and comprehensive to be admissible in a court of law. Certain additional aspects, such as, the source of the evidence, a legitimate witness, electronic evidence and data etc., can all add credibility to the case. In the absence of these, banks may not have the confidence to take legal recourse or action on the fraudster which could be one of the reasons why banks may not be reporting all the cases to law enforcement agencies.Prior to Satyam[71] (often called as India's Enron) fraud, most companies perceived fraud as largely an internal event, primarily pinching the bottom line. They now understand that fraud can have an impact not only on the reputation and business prospects but also on the survival of the firm. This concern has led to higher demand for FCAs in countries like India and China. The Ministry of Corporate Affairs in India has also established the Serious Fraud Investigation Office, which seeks the help of FCAs. The government recently proposed to give more teeth to the SFIO under the new Companies Bill by providing it statutory recognition and empowering it with more powers. The FCA's being professional members of the CG and Audit Committees, can play a far greater role in coordinating company efforts to achieve a cohesive policy of ethical behavior within an organization.[72]By helping companies to detect and prevent fraud, FCAs can create a 'positive' work environment, establish 'effective' lines of communication, and be vigilant as a corporate 'watchdog', the FCAs role can gradually evolve into a key component in the CG system.Let us hope that FCAs, through their specialized knowledge, training and skills, will be able to improve CG scenario, still a work-in-progress, across the globe.

Last, but not the least, effective customer education and communications programs–helping customers recognize how to prevent fraud, but also helping them understand their own responsibilities–should go hand-in-hand with sophisticated cyber security measures. Only by working in partnership with their customers can financial institutions develop truly effective fraud prevention efforts.

## ACKNOWLEDGEMENT

The author is grateful to the reviewer of this journal for carefully reading the paper and for offering his valuable comments and suggestions, which finally helped the author to improve this paper.

## REFERENCE

1. Singh, M.K. (2005). Bank Frauds—What Every Banker Needs to Know, *IBA Bulletin,* September, 3-7.
2. 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,* 4(12), December, 370-380.
3. Pan, S. (2015). An Overview of Indian Banking Industry, *International Journal of Management and Social Science Research*, Vol. 4, No. 5, May, 67-71.
4. Chakraborty, S. (2013). Indian banking set to become fifth largest by 2020: KPMG-CII Report, Business Standard News, September 13, 2013.
5. Kaveri, V.S. (2014). Bank Frauds in India: Emerging Challenges, *Journal of Commerce and Management Thought*, 5(1), 14-26.
6. KPMG (2012), India Fraud Survey, available at www.kpmg.
7. Chiezey, U. and Onu, A.J.C. (2013). Impact of Fraud and Fraudulent Practices on the Performance of Banks in Nigeria, *British Journal of Arts and Social Sciences,* 15(1), 12-25.
8. Deloitte Fraud Survey (2015), The Deloitte India Banking Fraud Survey Report Edition II. Available at www.deloittee.com/in.
9. Bhasin, M.L. (2016), Role of Technology in Combatting Bank Frauds: Perspectives and Prospects, *International Review of Social Sciences*, 4(1), 21-37.
10. Gates, T. and Jacob, K. (2009). Payments Fraud: Perception versus Reality, *Economic Perspectives*, 33(1), 7-15.
11. ACL Services Limted, Fraud Detection using Data Analytics in the Banking Industry," Discussion paper, available at www.acl.com/bankingfraud, 1-8.
12. Bhasin, M.L. (2016),The Creative Accounting Practices: An Experience of a Developing Economy, *International Journal of Management, Social Sciences Research,*5(4), April, 7-16.
13. Berney, L. (2008), "For online merchants, fraud prevention can be a balancing act", *Cards & Payments*, 21(2), 22-7.
14. Malphrus, S. (2009), Perspectives on Retail Payments Fraud", *Economic Perspectives*, 33(1), 31-36.
15. Wells, J. T. (2005). New Approaches to Fraud Deterrence, *The Chartered Accountant*, May, The Institute of Chartered Accountants of India, New Delhi, 1453-1455.
16. Institute of Internal Auditors (2009). International Professional Practices Framework, published by the IIA.
17. Freddie Mac (2015). Fraud Mitigation Best Practices, January, available at www.freddiemac.com.
18. Pasricha, P. and Mehrotra, S. (2014). Electronic Crime in Indian Banking, *Sai Om Journal of Commerce and Management*, 1(11), November.
19. Bhasin, M.L. (2012), Audit Committee Mechanism to Improve Corporate Governance: Evidence from a Developing Country, *Modern Economy*, 3(7), November, 856-872.
20. PwC (2014)Global Economic Crime Survey 2014
21. Dzomira, S. (2014), Cyber-banking fraud risk mitigation conceptual model, available at https://www.academia.edu.
22. Bhasin, M.L. (2015), Forensic Accounting: Perspectives and Prospects, *The Pakistan Chartered Accountant Journal*, Oct.-Dec., pp. 44-48.
23. Bhasin, M.L. (2011), Corporate Governance Disclosure Practices in India: An Empirical Study, *International Journal of Contemporary Business Studies*, 2(4), April, 34-57.
24. Bhasin, M.L. (2016), Communion of Corporate Governance and Forensic Accounting: A Study of an Asian Country, *British Journal of Research*, 3(1), Published by Pubicon International Publication, 14-40.

25. 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*, 2(7), 22-27 July.
26. Deloitte Survey (2012). Indian Banking Fraud Survey-2012, *Business Standard,* February 8.
27. 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.
28. Jeffords, R.; Marchant, M. L. and. Bridendall, P.H. (1992). How Useful Are The Tread Way Risk Factors? *Internal Auditor*, June, 60-62.
29. Calderon, T. and Green, B.P. (1994). Internal Fraud Leaves Its Mark: Here's How to Spot, Trace and Prevent It, *National Public Accountant,* 39(2), August, 17-20.
30. Ziegenfuss, D.E. (1996). State and Local Government Fraud Survey for 1995.*Managerial Auditing Journal*, Vol. 9, November, p.49.
31. Willson, R. (2006). Understanding the Offender/Environment Dynamics for Computer Crimes.*Information Technology and People,* 19(2), 170-186.
32. Bhasin, M.L. (2013) Corporate Accounting Fraud: A Case Study of Satyam Computer Limited, *Open Journal of Accounting*, April, 2(2), 26-38.
33. Bhasin, M.L. (2013) Corporate Accounting Scandal at Satyam: A Case Study of India's Enron, *European Journal of Business and Social Sciences*, 1(12), March, 25-47.
34. Ganesh, A. and Raghurama, A. (2008).Status of Training Evaluation in Commercial Bank-- A Case Study, *Journal of Social Sciences and Management Sciences*, 37(2), Sept.137-58.
35. Khanna, A. and Arora, B. (2009). A Study to Investigate the Reasons for Bank Frauds in Indian Banking Industry, *Int. Journal of Business Science and Applied Management*, 4(3), 1-21.
36. Mhamane, S. and Lobo, L.M.R.J. (2012), Fraud Detection in Online Banking Using HMM, Paper presented at "2012 International Conference on Information and Network Technology, " published in IPCSIT 37(1), 200-204.
37. Bhasin, M. L. (2016), The Fight Against Bank Frauds: Current Scenario and Future Challenges, *Ciencia e Tecnica Vitivinicola Journal*, 31(2), Feb., 56-85.
38. Bhasin, M. L. (2016), Debacle of Satyam Computers Limited: A Case Study of India's Enron, *Wulfenia Journal*, 23(4), April, 124-162.
39. Bhasin, M. L. (2016), Strengthening Corporate Governance through an Audit Committee: AnEmpirical Study, *Wulfenia Journal*, 23(2), 1-27.
40. Bhasin, M.L. (2011), Corporate Governance Disclosure Practices in India: An Empirical Study**,** *International Journal of Contemporary Business Studies (IJCBS),* 2(4), April, 34-57.
41. Bhasin, M.L. (2006). Data Mining: A Competitive Tool in the Banking and Retail Industries, *The Chartered Accountant*, October, 588-594.
42. ACFE (2012), "Report to the Nations 2012," The Association of Certified Fraud Examiners, available at www.acfe.com.
43. Inamdar, N., 2013. Fraud at public sector banks: A rampant occurrence. Business Standard. Available from www.business-standard.com.
44. RBI (2015), RBI issues framework for banks to deal with frauds, May 8. Available from http://www.livemint.com.

45. Bhasin, M. L. (2013). Corporate Governance and Forensic Accountant: An Exploratory Study, *Journal of Accounting*, *Business and Management*, October, 20(2), 55-75.
46. Pai, S. (2015), Banks No Safe Havens for Your Money; Depositors Lost Rs. 27,000 crore in Last Five Years, *DNA*, April 8.
47. Sen, A. (2015), KPMG's Latest Fraud Survey Kicks up Some Dangerous Statistics, available at www.allianceone mumbai.com.
48. Dubey, N., 2013. Banking frauds: Prevent or lament. Available from www.mondaq.com.
49. Bhasin, M.L. (2007). Forensic Accounting: A New Paradigm for Niche Consulting**,** *The Chartered Accounting Journal*, January, 1000-1010.
50. Mueller, K. (2015). How technology is shaping the fight against fraud? 25 February. Available at www.inc.com.,1-6
51. Bhasin, M. L. (2016). Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country, *International Business Management*, 10(4), 479-492.
52. Deloitte Fraud Survey, 2015. The Deloitte India Banking Fraud Survey Report Edition II, Press Trust of India Report Dated April 23, 2015.
53. Bhasin, M.L. (2007a). Mitigating Cyber Threats to the Banking Industry, *The Chartered Accountant,* April, 1618-1624.
54. Bhasin, M. L. (2015). Menace of Frauds in the Indian Banking Industry: An Empirical Study, *Australian Journal of Business and Management Research*, 4(2), April, 21-33.
55. Geffner, M. (2014). How banks fight fraud in electronic banking, May 29. Available at www.banrate.com. 1-2.
56. Bhasin, M.L. (2016), Integration of Technology to Combat Bank Frauds: Experience of a Developing Country, *Wulfenia Journal*, 23(2), Feb., 201-233.
57. Ernest & Young (2012). India Fraud Indicator 2012, a study by E&Y's Fraud Investigation and Dispute Services. Available at www.ey.com/india.
58. RBI (2015), RBI issues Framework for Banks to Deal with Frauds, May 8, available at http://www.livemint.com.
59. RBI (2015), RBI to Soon Issue Norms for Central Fraud Registry: Deputy Governor, Press Trust of India, March 29, 2015.
60. Hoffmann, A.O.I. and Birnbrich, C. (2012).The impact of fraud prevention on bank-customer relationships, *International Journal of Bank Marketing*, 30(5), 390-407.
61. Accenture Analytics Innovation Center (2015), "Protecting the Customer: Fighting Bank Fraud in a New Environment," available at https://www. accenture.com, 1-9.
62. Klein, R. (2015). How to Avoid or Minimize Fraud Exposures, *The CPA Journal*, March, 6-11.
63. 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.hindustan times.com.
64. Banks, D. G. (2004).The Fight against Fraud," *Internal Auditor*, Volume 62 (1), April, 62-66.Available at www.highbeam.com.
65. Chakrabarty, K.C. (2013). Inaugural Address, National Conference on Financial Fraud, organized by ASSOCHAM, New Delhi, July 26.
66. Siddique, M.I. and Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector: an overview, *International Journal of Business and*

*Information Technology*, 1(2), September, 159-164.
67. Bhasin, M.L. (2013), Audit Committee Scenario & Trends: Evidence from an Asian Country, *European Journal of Business and Social Sciences,* 1(11), February, 1-23.
68. ASSOCHAM (2015). Current fraud trends in the financial sector, joint study of Associated Chambers of Commerce and Industry of India, New Delhi, and PWC, June. Available at www.pwc.in/
69. Pasricha, P. and S. Mehrotra, 2014. Electronic crime in Indian banking. *Sai Om Journal of Commerce and Management*, November, 1(11),7-14.
70. Bhasin, M.L. (2011), Combating Cheque Fraud in Banks: The Role of Internal Auditor and Technology, *Siddhant,* Dec. 6, available at www.indianjournals.com.
71. Bhasin, M.L. (2013), Corporate Accounting Fraud: A Case Study of Satyam Computers Limited," *Open Journal of Accounting*, 2(4), April, 26-38.
72. 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,* 1(2), June, 11-52.

**Table1:** Types of Frauds Prevalent in the Indian Banking Industry

| Bribery and corruption | Cybercrime | Multiple funding | Counterfeit cheques |
|---|---|---|---|
| Terrorist Financing | Data Security | Identity theft | Tunneling |
| Money Laundering | Loan loss | Internet banking frauds | Absence of collaterals |
| Tax Evasion | Fraudulent documentation | Incorrect sanctioning | Mobile Banking Risks |

**Table 2:** 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)

**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 |

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

| Section | 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% |

(Source: Based on the findings of the questionnaire-based Survey)

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

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

(Source: Based on the findings of the questionnaire-based Survey)

**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 |

(Source: Based on the findings of the questionnaire-based Survey)

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

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

(Source: Based on the findings of the questionnaire-based Survey)

**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 |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 9:** Responses about the Key Reasons for Perpetration of Frauds in Banks

| 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 |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 10:** Responses about Detection and Prevention of Frauds in Banks

| Monitoring accounts manually | Training of Employees | Customer Education | Real-time decision-tools | Fraud detection techniques |
|---|---|---|---|---|
| 22% | 76% | 77% | 43% | 80% |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 11:** Response about How Fraud incident is Typically Detected in Bank

| Review by law enforcement agency | By accident | Through a third party notification | At the point of transaction | Through automated data analysis or software | During audit or reconciliation | Internal whistle-blower | By customer complaint |
|---|---|---|---|---|---|---|---|
| 4 | 6 | 7 | 10 | 16 | 18 | 18 | 21 |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 12:** Response about the Process Followed to Handle Fraud Incidents in Banks

| An internal investigation is carried out | Incident is reported to law enforcement agency | Individual in question is asked to resign | External investigation by an independent consultant |
|---|---|---|---|
| 46% | 32% | 14% | 8% |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 13:** Response about Technologies Used by Banks to Detect and Prevent Frauds

| Fraud management system | Strong authentication system | Intrusion Prevention technologies | Encryption System | Neural fraud detection systems |
|---|---|---|---|---|
| 78% | 62% | 85% | 68% | 70% |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 14:** Response about the Most Important Areas which are Crucial to an Anomaly Detection Solution

| Highlight Red flag areas | Areas controls needed | Tracking high-risk customers | Case management | Audit Trails |
|---|---|---|---|---|
| 29% | 27% | 19% | 13% | 12% |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 15:** Response about New Fraud Trends that will be of Concern in the Next Two Years

| ATM | Phishing/vishing | Mortgage | Credit card | Others |
|---|---|---|---|---|
| 23% | 16% | 14% | 10% | 37% |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 16:** Demand for Forensic Accountants in the Future

| Question | Mean | Standard Deviation |
|---|---|---|
| The demand for forensic accountants in the next 5 years will: | 4.46 | (0.646) |
| The demand for forensic accountants in the next 10 years will: | 4.34 | (0.651) |
| The demand for forensic accountants in the next 20 years will: | 4.20 | (0.728) |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 17:** Availability of Forensic Accountants in the Future

| Question | Percent |
|---|---|
| Will there be enough forensic accountants available to meet the demand in the next 5 years: | |
| Yes | 13 |
| No | 62 |
| Not Sure | 25 |
| Will there be enough forensic accountants available to meet the demand in the next 10 years: | |
| Yes | 25 |
| No | 29 |
| Not Sure | 46 |
| Will there be enough forensic accountants available to meet the demand beyond the next 10 years: | |
| Yes | 32 |
| No | 16 |
| Not Sure | 52 |

(Source: Based on the findings of the questionnaire-based Survey)

**Table 18:** Response about the Ratings of the Importance of the Software Tools for Forensic Chartered Accountants

| Tools | Mean | Standard Deviation |
|---|---|---|
| ACL | 5.45 | (1.297) |
| IDEA | 5.24 | (1.232) |
| Data Mining | 5.83 | (1.240) |
| Digital Evidence Recovery | 5.82 | (1.224) |

(Source: Based on the findings of the questionnaire-based Survey)