FRAUDS IN INDIAN BANKING & CYBER SECURITY ISSUES: AN ANALYSIS

Mrs. B. Mamatha
Research Scholar
Osmania University

Abstract:*Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a Financial Institution, or to obtain money from depositors by fraudulently posing as a bank or other Financial Institution. In many instances, bank fraud is a criminal offence. Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. in a computing context, security includes both cyber security and physical security. The present study is undertaken to know the banking frauds year wise and bank wise and various cyber security issues in India.*

The study is based on secondary data covering a period of 9 years i.e. 2004 to 2013 to reflect the number of frauds in Banking Sectors and Cyber Security issues during that period.

Introduction

India has a diversified Financial Sector undergoing rapid expansion, both in terms of strong growth of existing Financial Services firms and new entities entering the market. The sector comprises commercial banks, Insurance companies, non-banking financial companies, co-operatives, pension funds, Mutual Funds and other smaller financial entities. The banking regulator has allowed new entities such as payments banks to be created recently thereby adding to the types of entities operating in the sector. However, the Financial Sector in India is predominantly a banking sector with commercial banks accounting for more than 64 per cent of the total assets held by the Financial System.

The Government of India has introduced several reforms to liberalise, regulate and enhance this industry. The Government and Reserve Bank of India (RBI) have taken various measures to facilitate easy access to finance for Micro, Small and Medium Enterprises (MSMEs). These measures include launching Credit Guarantee Fund Scheme for Micro and Small Enterprises, issuing guideline to banks regarding collateral requirements and setting up a Micro Units Development and Refinance Agency (MUDRA). With a combined push by both government and private sector, India is undoubtedly one of the world's most vibrant capital markets.

The banking and financial services, government and public administration, and manufacturing industries were the most represented sectors in the fraud cases that were examined by Association of Certified Fraud Examiners while preparing the Global Fraud Study 2016. The frequency, complexity type and the money involved in banking frauds have increased manifold resulting in a very serious cause of concern for regulators, such as RBI. In the last three years, public sector banks (PSBs) in India alone have lost close to Rs. 22,700 Crores on account of banking frauds. This amount has been increasing with each passing year. In most cases we have the staff of the banks involved and in some cases it has been because of technological attempts by outsiders.

Evolution of frauds in banks

In the earlier times, the frauds were limited to fake currency circulation (some of which entered the banking system), forged cheques (again a case of duplicity and printing of fake security items like cheques, Demand drafts and Pay Orders) and advancing loans to known parties without checking the repayment ability and cash-earning proposition in the loan proposal(s). With the advent of technology, cybercrime has become the new menace of the day.

Definition

Fraud, under Section 17 of the Indian Contract Act, 1872, includes any of the following acts committed by a party to a contract, or with his connivance, or by his agents, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:

- The suggestion as a fact, of that which is not true, by one who does not believe it to be true;
- The active concealment of a fact by one having knowledge or belief of the fact;
- A promise made without any intention of performing it;
- Any other act fitted to deceive;
- Any such act or omission as the law specially declares to be fraudulent

Review of Literature

Anuj Sharma, Prabin Kumar Panigrahi(2012)[1] made a study to presents a comprehensive review of the literature on the application of data mining techniques for the detection of financial accounting fraud and proposes a framework for data mining techniques based accounting fraud detection. The systematic and comprehensive literature review of the data mining techniques applicable to financial accounting fraud detection may provide a foundation to future research in this field.

Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari(2013)[2] focus on cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure.

Chiezy and Onu (2013)[3] made a study to evaluated the impact of fraud on the performance of 24 banks in Nigeria during 2001-2011, using Pearson correlation and multiple regression analysis. They recommended that "banks in Nigeria need to strengthen their internal control systems and the regulatory bodies should improve their supervisory role."

Chandar H. Rohra(2013)4 made a study to analyse some issues related to the use of cyberspace for fraud by cyber scammers especially Financial Fraud and the techniques used. It will also provide an analysis of the existing legislative and regulatory framework and their efficiency in combating this form of cross-border crime taking India as a case study. It presents the historical origin of financial frauds and presents a small survey of some popular financial frauds committed in the recent years in India and ways to prevent frauds from happening.

Charan Singh (2016)[5]This study endeavors to cover issues such as banking frauds and mounting credit card debt, with a detailed analysis using secondary data (literature review and case approach) as well as an interview-based approach, spanning across all players involved in reporting financial misconduct. It proposes some recommendations to reduce future occurrence of frauds in Indian banking sector. The credibility of third parties such as auditing firms and credit rating agencies is also questioned in the study and is believed to be a significant contributor amongst other causes, such as oversight by banks and inadequate diligence.

Dr. Sukhamaya Swain, Dr. Lalata K Pani (2016)[6] made a study on various aspects of frauds in Indian banking system. It evaluates the statistics involved with fraud basis secondary data available from reliable sources and also analyses the same. Each of the types namely KYC related, loan related and technological aspects are discussed in details along with the reasons. At the end, some suggestions are placed for banks to practice.

Charan Singh , Deepanshu Pattanayak(2016)[7] the present study endeavours to cover issues such as banking frauds and mounting credit card debt, with a detailed analysis using secondary data(literature review and case approach) as well as an interview-based approach, spanning across all players involved in reporting financial misconduct. The report touches upon the case of rising NPAs in the past few years across various scheduled commercial banks, especially public sector banks. The study finally proposes some recommendations to reduce future occurrence of frauds in Indian banking sector.

Reurink, Arjan(2016)[8] it describes the different forms of fraudulent behavior in the context of financial market activities, the prevalence and consequences of such behavior as identified by previous research, and the economic and market structures that scholars believe facilitate it. To structure the discussion, a conceptual distinction is made between three types of financial fraud: financial statement fraud, financial scams, and fraudulent financial mis-selling. What emerges is a picture of financial fraud as a complex phenomenon that can take very different forms, depending on the market segments in which it occurs, the financial instruments it pertains to, and the actors involved.

Research Gap

The review of literature points out that the studies are based on banking frauds and mounting credit card debt, different forms of fraudulent behavior in the context of Financial Market activities, cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. Hence, the study is undertaken to know the various frauds in banking industry and cyber security issues.

Objectives of the Study

The objectives of the study are

- To analyse the cyber frauds year wise and group wise
- To suggest appropriate and suitable measures of cyber security issues.

Sources of Data

The study is based on secondary data. The Secondary data sources include Annual Reports of RBI, Research Publications, News papers, PWC Manuals and Websites.

Period of the Study

The study covers a period of 9 years from 2004 to 2013 i.e. online reporting and monitoring of fraud cases by the bank has been in place since May 2004.

Bank Frauds Year wise and Group Wise

Year wise fraud cases reported by commercial banks are shown in table-1

Table: 1

Year wise fraud cases reported by commercial banks

(No. of cases in absolute terms and amount involved in Rs. Crore)

Amt Involved	< Rs 1 lakh		> 1 lakh and up to Rs 1 crore		> Rs 1 cr and up to Rs 50 crore		> Rs.50 crore		Total Fraud cases	
FY (Apr–Mar)	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount
Pre-2004	2292	4.24	819	96.65	613	2951.64	13	1244.26	3737	4296.80
2004–05	7553	12.50	2407	287.32	111	584.89	1	53.57	10072	938.29
2005–06	11395	18.63	2334	290.20	192	1009.23	2	135.47	13923	1453.53
2006–07	20415	31.22	3048	325.02	158	791.17	1	78.45	23622	1225.86
2007–08	17691	30.25	3381	383.98	177	662.31	–	–	21249	1076.54
2008–09	19485	33.85	4239	442.94	214	1129.56	3	305.33	23941	1911.68
2009–10	20072	30.36	4494	474.04	222	1129.28	3	404.13	24791	2037.81
2010–11	15284	26.09	4250	494.64	277	1515.15	16	1796.20	19827	3832.08
2011–12	10638	19.05	3751	509.17	327	2113.23	19	1650.08	14735	4491.54
2012–13	9060	22.11	3816	491.13	372	2798.00	45	5334.75	13293	8646.00
Total	133885	228.31	32539	3795.10	2663	14684.46	103	11202.25	169190	29910.12

Source: www.rbi.org

From the above table it is clear that the no of cases increased from 2004-2006 whereas in the year 2007-08 it was decline to 17691 cases due to financial crisis thereafter there is an increasing trend till 2010 and from the year 2010-2011 it was decline because the awareness is created regarding cyber security where as in case of more than 1crore and up to 50 Crore cases there is continuous increase in number of cases as there are using online business and e-Commerce.

Year wise details of fraud cases closed

The no of fraud cases closed year-wise is shown in table-2

Table-2

Year wise details of fraud cases closed

(No. of cases in absolute terms and amount involved in Rs. Crore)

Amt Involved	< Rs 1 lakh		> 1 lakh and up to Rs 1 crore		> Rs 1 cr and up to Rs 50 crore		> Rs.50 crore		Total Fraud cases	
FY (Apr–Mar)	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount
Pre-2004	1661	2.85	568	36.33	11	94.64	1	85.66	2241	219.48
2004–05	6047	8.47	470	33.27	13	99.68	–	–	6530	141.42
2005–06	11611	9.47	154	10.86	11	75.93	1	55.28	11777	151.54
2006–07	14291	9.46	248	17.53	4	34.30	–	–	14543	61.29
2007–08	12861	11.23	374	26.79	3	32.05	–	–	13238	70.07
2008–09	6796	9.25	420	20.84	10	49.28	–	–	7226	79.37
2009–10	5828	8.99	636	38.03	4	21.18	–	–	6468	68.20
2010–11	13526	13.47	649	42.88	7	14.26	–	–	14182	70.61
2011–12	38330	23.58	756	49.80	10	33.04	–	–	39096	106.42
2012–13	11198	8.45	556	35.83	14	78.51	–	–	11768	122.79
Total	122149	105.22	4831	312.16	87	532.87	2	140.94	127069	1091.18

Source: www.rbi.org

From the above table it is clear that more than 90% of the cases are closed every year in all the categories because the central bank said that the fraud cases can be closed where the investigation is on or challan / charge sheet has not been filed in the Court for more than three years from the date of filing of First Information Report by the CBI / Police; or the trial in the courts, after filing of charge sheet / challan by CBI / Police, has not started,

Bank Group wise fraud cases reported as of 31-Mar 2013 are shown in table-3

Table-3

Bank Group wise fraud cases

(No. of cases in absolute terms and amount involved in Rs. Crore)

Amt Involved	< Rs 1 lakh		> 1 lakh and up to Rs 1 crore		> Rs 1 cr and up to Rs 50 crore		> Rs.50 crore		Total Fraud cases	
Bank Group	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount	No. of cases	Total Amount
Nationalised Banks including SBI Group	7622	31.97	19753	2847.11	2184	11867.24	94	10061.69	29653	24828.01
Old Pvt. Sector Banks	622	2.38	1463	225.09	181	1001.56	5	478.68	2271	1707.71
New Pvt. Sector Banks	83850	112.36	6984	510.18	225	1445.82	1	72.11	91060	2140.47
Sub Total (Private Banks)	84472	114.74	8447	735.27	406	2447.38	6	550.79	93331	3848.19
Foreign Banks	41791	81.60	4339	212.72	73	369.84	3	569.76	46206	1233.92
Grand Total	133885	228.31	32539	3795.10	2663	14684.46	103	11202.25	169190	29910.12

Source: www.rbi.org

From the above table it is clear that less than 1 lakh cases are more in cases of private sector According to data released by the RBI as on June-end 2011, PSBs accounted for 74.6% of bank deposits while private sector banks had only 18%, with the rest of the funds lying with regional rural banks and foreign banks. Interestingly, it is the private banks, including foreign banks, which stand for perfection and are known for prompt service that appear to be more prone to banking frauds.SBI reported 784 cases involving Rs 298 crore for the year 2010-11, the RTI query revealed.

ICICI Bank alone accounted for almost half of the frauds reported to the RBI. Of the 5,319 cases reported in the current financial year (till September) by 29 private banks, a whopping 3,304 were from ICICI.

FRAUDS IN INDIAN BANKING AS ON 2018

Until now 2018 has seen a string of bank frauds and scams across India and has raised questions about the governance and credit managing practices at private and public sector banks. The Frauds in Indian banking sector are shown in Table-4

Table-4

Frauds in Indian Banking Sector as on April 2018

S. No:	Year	Scam name	Scammer Name	Scam Amount
1	2011	PNB scam	Nirav Modi	Rs 11,400 crore
2	2015	R P Infosystem scam	Shivaji Panja and Kaustav Ray	Rs 180crore
3	2018	PNB scam	Nirav Modi	Rs 91 million
4	2018	SBI fraud case	Kanishk Gold Pvt Ltd (KGPL)	Rs 824.15 crore

5	2018	Karnataka Bank fraud case	Mehul Choksi	Rs 86.47 crore
6	2018	Rotomac Case	Vikram Kothari	Rs 3,695 crore
7	2018	United Bank of India case	Archana Bhargava	Rs 3.6 crores

Source: www.ibtimes.co.in

From the above table it is clear that by the end of April 2018 maximum frauds has taken place. The biggest scam was PNB Scam with an amount of Rs 91 Million.

Cyber Security Issues

Financial sector faced almost three times the cyber attacks as compared to that of the other industries

- Data breaches (both internal through fraud and external through cyber criminals) leads to the exponential rise in costs
- It has been estimated that cost of implementing and managing the cyber security infrastructure will increase over 40% by 2025
- There is an increase in biometrics and tokenization as banks have begun to recognize that in addition to being a solution for payments these controls are also useful in security the sensitive data
- Customers are using biometrics for banking activities such as authentication for mobile banking, transaction at ATMs and payments
- With digital channels becoming the preference choice of customers for banking services, banks will also need to leverage advanced authentication and access control processes, without any compromise to customer experience

Regulatory Perspective

➢ To ensure security in banking industries, the Reserve Bank of India removed a **Circular DBS.CO.ITC.BC.No.6/31.02.008/ 2010-11** dated **April 29 2011**, where all banking institutions have to comply for. Some of the key features of the regulations are:
➢ Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank
➢ Arrangement for continuous surveillance
➢ Comprehensive network and database security
➢ Protection of customer information
➢ Cyber security preparedness indicators
➢ Cyber Crisis Management Plan
➢ IT architecture should be conducive to security
➢ An immediate assessment of gaps in preparedness to be reported to RBI
➢ Cyber security awareness among stakeholders/ Top Management/ Board

Security Considerations

1. **Internet Banking**: Security controls like multi factor authentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered.
2. **Mobile Banking**: It should be ensured that mobile applications are up to date and should be tested. Latest hardening standards could be implemented.
3. **Wallet Transactions**: Awareness material on Phishing, Malware attacks, vishing and social engineering, Password security etc. should be incorporated.
4. **ATM Security**: Biometrics like eye-retina, voice scan or fingerprint scan should be introduced by Banks.
5. **UPI (Unified Payment Interface)** : Banks and PSPs need to think through their security strategies, governance models and predictive controls to build a secure UPI environment that ensures a seamless user experience and at the same time balances security risks.

Cyber Security Trends to Look Out for in 2017 India

The prime Minister of India Narendra Modi has identified cyber security as one of the key areas of development in India. Considering the rapid growth of cyber trends including mobile transactions, e-commerce, and the evolutionary Digital India, cyber security has become crucial. No matter what the economical dimensions of business companies are, deployment of effective cyber security is mandatory to prevent cyber attacks and threats. Hence, the IT analysts and strategists have come up with various cyber security trends to look out for this year

1. Demonetisation and Digital Payments: The focus on digitalised payments and demonetisation has naturally propelled the working of cyber security experts. Since, digital payments through ATM cards, mobile wallets, debit/credit cards and online banking are not equipped with proper cyber-attack protection, 2017's main target now lies in securing digital payment methods.
2. Potent Malware: Malware still lies as one of the main enemies of digitalisation. With Modi's aim of achieving a cashless India, malware easily puts a setback. With Botnet Cleaning Centre and Malware Removal Centre, the threats could be receded down considerably.
3. Protection of Infrastructure : The Indian government, at the beginning of this year, has suggested the improvement of infrastructure protection. It has been quite some time that the government is keenly formulating the necessary guidelines and regulations for its effectiveness. The National Critical Information Infrastructure Protection Centre (NCIIPC) under the government has proposed its implementation.
4. Aadhaar card: security Violation of basic civil liberties such as data protection and privacy protection occur on a daily basis that puts a severe setback. Indian government failed to take the necessary security measures for violation of civil liberties and cyber security regarding Aadhaar card and digitalisation. Hence, it has become a critical necessity.
5. International cyber security: It is imperative to realize the internationality of cyber security and cyber attacks. The Indian government has still not implemented any globally acceptable law for cyber security or cyber security treaties.
6. Medical security: Over the past decade, the importance of ICT (Information and Communication Technologies) has greatly increased in medical services. Last year, the government failed to provide complete cyber security, data and privacy protections for medical organizations.

7. Cyber insurance and litigations: The reason behind the lack of development in cyber security is the dearth of awareness. The better half of 2017 has already focused on spreading cyber awareness. Governmental law enforcement agencies must execute efficient cybercrime investigations and cyber forensic abilities. Also, due to the growth of cyber-attacks, this year expects greater cyber security insurance.
8. The fault of encryption: The fact that encryption is present and available everywhere makes it exceedingly hard for cyber inspection yet makes it easier for cybercriminals to creep in. Security programmes should condense the mass network and immediately identify security records after a code has been decrypted.
9. Increase in social attacks: Attacks through email or text messages are nothing new: coaxing the user into believing that he/she has won an outstanding offer via email. The users often, not sensing the trap, click on the malicious link that subsequently leads them to ransom ware.
10. Security of IoT: Internet of things still lacked the essential cyber security and cyber protection methods in 2016. Although it has not yet completely evolved, 2017 aims for maximum IoT protection

Findings

- Cyber attacks in the country caused financial damages to the tune of about USD 500,000 to India companies.
- The Cisco 2018 Annual Cyber security Report shows that 50 per cent of organisations in India are reliant on automation, 53 per cent are reliant on machine learning and 51 percent are highly reliant on artificial intelligence.
- During 2010-11, the ICICI and HSBC banks put together have reported 13,067 cases. SBI tops the list of PSBs with the highest number of fraud cases reported in the current financial year.
- In the year 2010-11, ICICI reported 10,684 of the total 19,845 cases. The second highest numbers of cases were reported by HSBC at 2,383 for the same period.
- 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 Rs2,500 crore every year.
- Digital payments through ATM cards, mobile wallets, debit/credit cards and online banking are not equipped with proper cyber-attack protection, 2017's main target now lies in securing digital payment methods.
- Mobile transactions (banking, shopping, paying bills, etc.) are growing exponentially. If we talk about only India, startling fact that over 72 crore transactions were done using mobile banking in 2016-17. This is a mammoth jump from 9.47 crore in 2013-14.

Suggestions

The Government should provide well defined citizen awareness programs aimed at preventing cybercrime as a proactive mitigation. Cybercrime awareness shall be introduced in academics in the early stages of education as a mandate for all the state and central, and public and private schools. Mechanisms shall be established for independent monitoring of awareness program at regular intervals to evaluate the number of people/regions covered. Awareness material shall be updated regularly to cover up-to-date information.

Conclusions

- ✓ India will witness a 65% rise in mobile frauds by 2017 as 40-45% of financial transactions are done via mobile devices, according to a joint study by ASSOCHAM.
- ✓ Cyber security is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, eco nomics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law. In practice, although technical measures are an important element.
- ✓ Cyber security is not primarily a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Furthermore, what is known about cyber security is often compartmented along disciplinary lines, reducing the insights available from cross-fertilization.
- ✓ This year has seen a string of bank frauds and scams across India that has raised questions about the governance and credit managing practices at private and public sector banks

Keywords

- ✓ PSBs-Public Sector Banks
- ✓ RBI- Reserve Bank of India
- ✓ ICT- Information and Communication Technologies
- ✓ IOT- Internet of Things

References

1. Anuj Sharma, Prabin Kumar Panigrahi, "A Review of Financial Accounting Fraud Detection based on Data Mining Techniques" International Journal of Computer Applications,2012 Vol 39,No 1,Pages 37-47.
2. Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, "Cyber Crime and Security"International Journal of Advanced Research in Computer science and Software Engineering,2013, Vol 6,Issue 4,,Pages 46-52.
3. Chiezy and Onu," Impact of Fraud and Fraudulent Practices on the Performance of Banks in Nigeria",British Journal of Arts and Social Science,2013Vol 15 ,No 1,Pages 12-28
4. Chandar H. Rohra,"an Insight of Evolution of Financial Frauds in India" Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal,2013,Vol 2 ,Issue 2.
5. Charan Singh (2016)" Frauds in the Indian Banking Industry", IIMB-WP N0. 505.
6. Dr. Sukhamaya Swain, Dr. Lalata K Pani,," Frauds in Indian Banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures",International Journal of Business and Management Invention,2016,vol 5,Issue 7,pages 1-9
7. Charan Singh , Deepanshu Pattanayak(2016)," Frauds in the Indian Banking Industry", IIMB-WP N0. 505
8. Reurink, Arjan(2016) Arjan Reurink (2016)," Financial Fraud: A Literature Review",Discussion paper 16/5

Websites

1. www.rbi.org
2. www.pwc.org

3. www.equifax.co.in
4. https://economictimes.indiatimes.com
5. https://www.businesstoday.in