"Framework for Early Detection of Banking Frauds"

[1]**Ankur Khairwal,** Research Scholar, National Forensic Sciences University
[2]**Dr. S. O. Junare,** Director - IFS, National Forensic Sciences University
[3]**Dr. Haresh Barot,** Associate Professor- IMT, National Forensic Sciences University

Article Info
Volume 83
Page Number: 6604 - 6609
Publication Issue:
July-August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June2020*
Publication: *10 August 2020*

Abstract

Banking industry in India has been under serious transformations in past two decades. Introduction of net banking, mobile banking and Artificial Intelligence has changed the perception of customers and their expectations. But in recent past continuous rise in banking frauds has been observed and that had a serious impact on India's economy. Bank fraud is an act of crime with a motive of obtaining money or assets by fraudster by exploiting vulnerabilities. Cyber-Crime is the new face in banking frauds and with the rise of internet and mobile technologies, incidents of cybercrime has grown significantly as users in India are still new to this digital means of banking. This paper is an attempt to explore banking fraud incidents in recent times and to explore approaches to detect such cases. Finally a framework has been developed to facilitate early detection of fraud in banking operations. On successful implementation this framework shall add value to banking operations.

Keywords: *Banking frauds, cybercrime in banking, Fraud Control Framework;*

Introduction

Indian banking sector has undergone rapid transformation in recent years and information technology has been a significant facilitator. Banking is now more centralized with the introduction of Core Banking Solutions (CBS) and various financial services are provided in an integrated manner using means like card-based payments and Electronic Clearing Services (RTGS/NEFT). Many services like Automated Teller Machine (ATMs), Internet and Mobile Banking has transformed banking operations and improved customer experience. Digital India campaign launched by Government of India in year 2015 has facilitated grownth of Digital wallets and UPI apps in India shown in Table 1.

Wallets by Bank	Telecom Industry Wallets	Independent Wallets
• ICICI Pockets • State Bank Buddy • Vodafone M-Pesa • Yono by SBI • ICICI Pockets • HDFC PayZapp	• Airtel money • Jio Money • mRupee • Trupay • MomoXpress • Ezetap	• Paytm • BHIM App • PhonePe • Mobiwik • FreeCharge • Oxigen

Table 1. Digital wallets and UPI apps in India

There has been a steady growth in total business and profits for banking sector in India, but there has been a significant rise in amount involved in frauds in Indian banking sector[1][2][3]. This results in serious impacts on overall performance of banks and is a matter of concern for all the stakeholders including regulators, customers, and banks. These bank frauds are sophisticated and innovative in terms of pattern of execution and amount involved in very huge [6]. This unhealthy development is a serious risk for the banks and it also affects their credibility substantially. India's financial systems are not self-reliant and are vulnerable, as they are dependent on international banking networks like Swift to make transactions. Banking Frauds in India can be classified into the following four categories though some cases found recently may match with more than one of them.

- **Exploiting the loopholes in the system:** Fraudsters generally plan well by doing research about banking operations and identifying vulnerabilities. In majority of the cases it has been found that fraudsters keep an eye on new changes in banking operations and studies the gaps resulted from new changes in the system and tried to exploit them [1][2].
- **Collusion between the insiders and the fraudsters:** Weak internal controls and lack of rotation of employees creates opportunity for collusion and is exploited by fraudsters [1].
- **Wilful defaulters:** According to the RBI, a wilful default is deemed to have occurred in any of the following four circumstances:
    1. Intentionally not repaying the loan though borrower has capacity to repay.
    2. Funds have been diverted for other purposes and not utilised for the stated purpose.
    3. Funds have been diverted and misused.
    4. Asset bought have been sold off without informing bank/lender.
- **Hackers** create clones of cards having details of users using skimmers and keyboard cameras on ATMs machines. Other cases of hacking involve calling people and tricking them into handing over information [9][10].

Literature Review

The RBI in its report states that among bank groups, Public sector banks (PSBs) which constitute the largest market share in bank lending, have accounted for the bulk of frauds reported in 2018-19. It was followed by private sector banks and foreign banks as shown in Table 1.

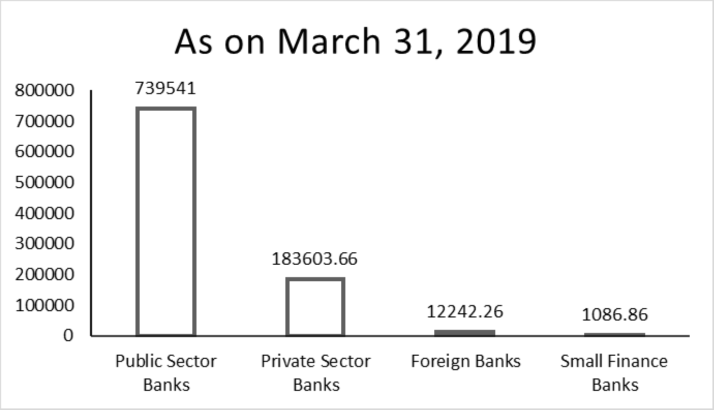

Table 2. Net NPA of Banks in India (amount in Crores)

The report also pointed out that the credit growth remained muted while the health of Public Sector Banks continued to decline. Based on the Case studies on banking frauds it is clear bank employees are involved in collusion practices with outsiders to commit banking frauds. Regulators and other government bodies are upgrading proper legal channel to combat banking frauds on regular basis but the implementation lacks effectiveness. In many cases it was observed that banks don't disclose frauds as it may damage bank's reputation. Most common reasons for increase in bank frauds are ignorant attitude of banking officials, pressure of meeting targets, and procedural delay in detection and reporting of frauds [4]. It was observed that employee’s lacks clear perception towards bank frauds and its impacts. Employee's consider compliances as formality and often fails to adhere. Beside these other reasons responsible for banking frauds are poor employment practices and lack of effective employee training. Bank employees are usually over-burdened with work and with weak internal control systems, and low compliance levels on the part of Bank Managers, Offices and Clerks the scenario becomes more vulnerable to frauds.

RBI in its recent report listed reasons for delay in detection of fraud cases [11]. These are,

- failure in identification and monitoring of Early Warning Signals (EWS) by banks
- failure in detection of EWS during internal audits
- Non-cooperative attitude of borrowers during forensic audits
- Inconclusive audit reports and lack of decision making in Joint Lenders' meetings

Based on the categories mentioned in section I and literature review, variants of banking frauds has been studies and 14 fraud types [8] with cases are presented in Table 3.

Sr. No	Fraud Type	Description	Case
1	Accounting fraud	Tampered accounting records are used to obtain loans	Satyam Scam [12]
2	Demand draft fraud	Demand draft credited to unknown account	UCO Bank Fraud Case [13]
3	Uninsured deposits	Bank offering public deposits that are not insured	PMC Bank Crisis [13]
4	Bill discounting fraud	After gaining bank's trust, company requests up front bill payments that it will collect from the customers later	ABC Cotspin Fraud case [13]
5	Duplication or Card skimming	Use of card skimming machines and a camera to capture card data and pin	Parvesh Dagar case [13]
6	Cheque frauds	Misuse of a cheque for example cheque kitting and Stolen checks.	Woman from Laxmi Nagar got message from the bank that Rs 1.10 crore was withdrawn from her account using two cheques.
7	Forged Document fraud	A person or an entity uses forged documents for availing any form of services from financial institutions.	PMC Bank Fraud case[14]
8	Loans and advances frauds	A borrower declares bankruptcy after taking a loan. Ex. fraud loan that hides the creditworthiness of the borrower	ABG Shipyard, Ruchi Soya Industries [13]
9	Money laundering	Scam where the true origin or the source of the fund is hidden for availing an unlawful benefit.	YES Bank Fraud [13]
10	Identity theft and Technology frauds	Illegal gain availed by using technology like misusing personal information of individual to obtain identity cards, accounts etc. and using this for availing benefits from a financial institution.	RBI has registered 921 cases of fraud based on net-banking and cards during April-September 2018 period [13]

11	Phishing, Vishing and Internet fraud	Using spam e-mails, tele calls, forged websites to get user information to steel money from their accounts.	Fruit vendor debit card update fraud [13]
12	Rogue traders	Trader engages in unauthorized trading to recover the loss from earlier trades by influencing internal controls.	Harshad Mehta, Navinder Singh Sarao [13]
13	Wire fraud	Falsified activity involving electronic means.	Hitesh Madhubhai Patel [14]
14	Clerical and accounting frauds	Oversight and manipulation of the facts in financial statement to get loan.	Punjab National Bank Scam[13]

Case Study - DHFL fraud case

India's leading bank Punjab National Bank (PNB) reported a loan fraud involving Dewan Housing Finance Limited (DHFL) to RBI. Report mentioned DHLF as a Non Performing Assest(NPA) with a loan of Rs 3,688.58 crore. Dewan Housing Finance Limited (DHFL) has abused crores of public money through various means like secured and unsecured loans and advances to shell companies, round tripping, tax avoidance and insider trading [15]. Money has routed through fake companies parked outside India, to acquire assets. The PNB has made provisions of Rs 1,246.58 crore in this case and is DHFL is currently under bankruptcy proceedings..

Fraud Control Framework

Fraud detection is a big challenge for ever changing banking sector. Banking sector needs to balance technology innovations with adequate controls to address multiple fraud-related challenges [5]. Current scenario of rising fraud incidents and amount involved indicates ineffectiveness of fraud risk management measures that needs improvement. Proposed Fraud Control framework is an attempt to improve risk management practices and minimize the impacts of frauds in banking sector. Fraud Control framework is a conceptual framework based on proactive real time monitoring of banking operations to facilitate early detection of fraudulent practices and continuous enhancement of fraud management practices. Traditional Fraud Life cycle [7] has eight components and proposed Fraud Control framework aims to enhance the capabilities of phases with introduction of a central component shown in figure 3.

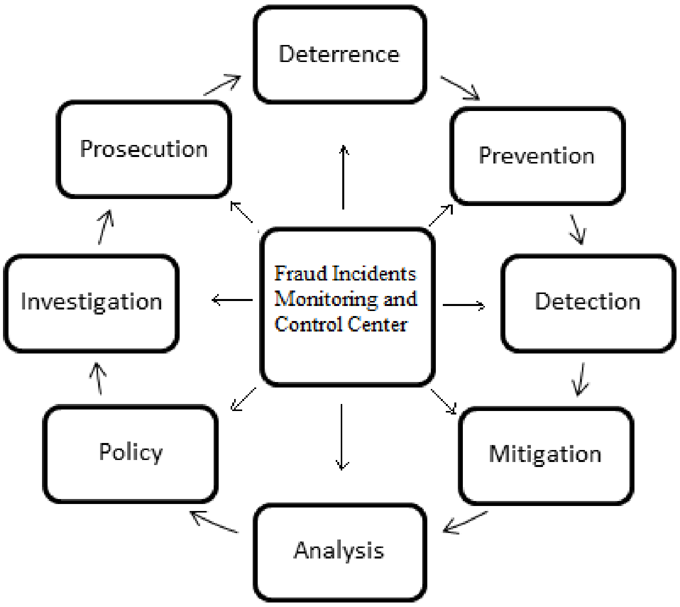

Figure 3. Fraud Control Framework

Components of Fraud Control Framework

Proposed Fraud Control Framework has nine components with Fraud Incidents monitoring and control centre being the central that works along with other eight components to provide effective control on fraud incidents. The objectives and guidelines of these nine components are mention below.

- **Fraud incidents monitoring and control centre (FIMCC)** plays most critical role with objectives to have real time monitoring of financial transactions and operational transactions committed in the banking system. All exceptional transactions need to be marked for investigation. This component closely work in coordination with other eight components and provide necessary inputs as and when required.
- **Deterrence** component is focused on proactive approach and may include best practices prevent fraud before it is attempted or discourage the attempt at fraud, for example, dual controls for all banking operations and fraud awareness training programs. Deterrence component can regularly update its control practices with inputs from FIMCC based on recent fraud incidents to strengthen Deterrence controls.
- **Prevention** component involves control practices to prevent fraud from occurring with the use of multi-factor authentication and authorization controls. Additional security controls like cryptography and firewalls also contribute as prevention. Dual controls for all activities can make preventive controls more effective. Preventive controls need to cover all type of frauds happened in past. Prevention component can take real time inputs from FIMCC on various fraudulent attempts on banking system and regular update on preventive controls can further harden the system.
- **Detection** component is based on reactive approach and includes statistical monitoring programs used to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity. The objective here is to detect presence of fraud or a fraud attempt. Detection makes use of analytical techniques like classification, statistical parameter calculation, numbers stratification, joining random diverse sources, duplicate testing, gap testing, entry date validation and numeric values summation. Detection component works closely with FIMCC and use of advance data analytics and techniques like Artificial Intelligence and big Data Analytics can make this more effective.
- **Mitigation** component is focused on minimizing the impact of fraud by stopping a fraudster from continuing or completing fraud, for example blocking an account. Mitigation component can take real time inputs from FIMCC to take quick action against fraud incident that can significantly minimize the impact of fraud.
- **Analysis** component is focused on reviewing losses and performing root cause analysis. Analysis can facilitate and help FIMCC to take note of fraud incidents and their root causes to help strengthen deterrence, prevention and detection components.
- **Policy** component aims to enhance governance practices by activities to evaluate, direct, monitor and assist in the deployment of policies to reduce the incidence of fraud. FIMCC can contribute to update policy and accountability can be enhanced through the past cases while maintaining the flexibilities of the banking needs. Banking codes and ethics too can be updated for example transaction over a certain limit to be reported.
- **Investigation** component includes forensic practices focused on obtaining evidence related to fraudulent activity. This further might lead to recovery of assets, but primarily provide enough evidence and support for the successful prosecution and conviction of the fraudster(s). Investigation component can take important inputs from FIMCC to effectively obtain evidence related to fraudulent activity.

- **Prosecution** component includes asset recovery, compensation, and conviction to fraudster. FIMCC can take inputs and use them to enhance effectiveness of other components.

Approval and support and of top management is critical for successful implementation of proposed framework. Skilled professionals are required to operate FIMCC to deliver expected value.

Conclusion

Fraud is prevalent issue within the banking sector and is bound to increase as the risks of fraud increases every day. This increase can be attributed to rapid development of technology, more competitive markets and an increase in globalisation. With fraud activity increasing at a rapid pace and costing banks crores of rupees every year, there is an imperative need of an effective framework to control fraudulent practices as early as possible. Proposed framework can facilitated real time monitoring and can contribute in continuous enhancement of fraud control practices.

References

[1]. Anthala, H. R. (2014). Research paper on Case laws of Fraud, forgery, and Corruption in Banks and Financial Institutions in India. IOSR Journal of Economics and Finance, 3(6), 53-57. doi:10.9790/5933-03653573

[2]. Kundu, s., &Rao, n. (2014). Reasons for banking fraud - a case of Indian public sector banks. International Journal of Information Systems Management Research & Development, 4(1), 11-24.

[3]. Gupta, P. K., & Gupta, S. (2015). Corporate frauds in India – perceptions and emerging issues. Journal of Financial Crime, 22(1), 79-103. doi:10.1108/jfc-07-2013-0045

[4]. Singh, T., & Nayak, S. (2015, August). Frauds in Banking. Retrieved from https://tejas.iimb.ac.in/articles/Banking%20Frauds_Tejas_Jan2016.pdf

[5]. Swain, D. S., &Pani, D. L. (2016). Frauds in Indian Banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures. International Journal of Business and Management Invention ISSN, 5(7), 01-09.

[6]. Bhasin, M. L. (2016). Frauds in the Banking Sector: Experience of a Developing Country. The East Asian Journal of Business Management, 4(4), 8-20. doi:10.20498/eajbe.2016.4.4.8

[7]. Wilhelm, Wesley Kenneth. “The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management.” (2004).

[8]. Frauds – Classification and Reporting: RBI (01-Jul 2015).

[9]. ASSOCHAM (Ed.). (2015). Current fraud trends in the financial sector, joint study of associated chambers of commerce and industry of India. New Delhi: PWC. Retrieved from www.pwc.in

[10]. Dzomira, S.(2015). Cyber-banking fraud risk mitigation: Conceptual model. Banks and Bank System, 10(2), 7-14.

[11]. Annual report of Reserve Bank of India (RBI) 2019-20 https://m.rbi.org.in/Scripts/AnnualReportPublications.aspx

[12]. M. Lal Bhasin, "Corporate Accounting Fraud: A Case Study of Satyam Computers Limited," Open Journal of Accounting, Vol. 2 No. 2, 2013, pp. 26-38. doi: 10.4236/ojacct.2013.22006.

[13]. Timesofindia.Indiatimes.com

[14]. Hindustantimes.com

[15]. Ndtv.com July 10, 2020, https://www.ndtv.com/business/pnb-dhfl-fraud-punjab-national-bank-reports-rs-3689-crore-dewan-housing-dhfl-loans-as-fraud-2260219