



**SONOPANT DANDEKAR ARTS, V.S. APTE COMMERCE
AND M.H. MEHTA SCIENCE COLLEGE, PALGHAR**

Department of Banking & Insurance

PROJECT REPORT

Third Year Banking & Insurance

Academic Year 2022-2023

Prepared by
Department of Banking & Insurance
Sonopant Dandekar Arts, V.S. Apte Commerce and
M.H. Mehta Science College, Palghar

INDEX

Sr. No.	Content
1	Notice for Project Submission
2	Curriculum where course (subject where project work/ field work is required)
3	List Learners with Project titles
4	Sample Projects



Sonopant Dandekar Shikshan Mandali's
Sonopant Dandekar Arts,
V. S. Apte Commerce &
M. H. Mehta Science College, Palghar

Estb.: 14 August 1968

Dr. Kiran Save, Principal

Kharekuran Road, Palghar (W), Tal. & Dist. Palghar,
Maharashtra - 401 404, INDIA
Tel. : +91 - 2525 - 252163
Principal : +91 - 2525 - 252317
Email : sdscollege@yahoo.com
Web. : www.sdscollege.com

Ref No.:

Date : 03/04/2023

Notice

Department of Banking & Insurance

This is to inform you that all the **Third Year Bachelor of Banking & Insurance** students are required to submit the hard copy of your final project report by **12th April 2023**. All submissions should be made to the **BBI Department, BMS Building** during office hours from 09.30 am to 01.30 pm. Ensure your report is properly.

S.S. Mishra

(Dr. Shreya Mishra)
HOD
Department of BBI

K. Save

Dr. Kiran J. Save
Principal

PRINCIPAL
Sonopant Dandekar Arts College,
V.S. Apte Commerce College &
M.H. Mehta Science College
PALGHAR (W.R.)
Dist. Palghar, Pin-401404

UNIVERSITY OF MUMBAI

No. UG/7 of 2018-19

CIRCULAR:-

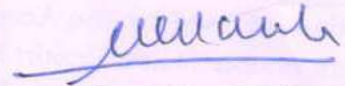
Attention of the Principals of the affiliated Colleges and Directors of the recognized Institutions in Commerce & Management Faculty is invited to this office Circular No.UG/121 of 2016-17, dated 27th October, 2016 relating to syllabus of Bachelor of Commerce (B.Com.) degree course.

They are informed that the recommendations made by the I/c Dean, Faculty of Commerce & Management in Banking and Finance at its meeting held on 28th February, 2018 have been accepted by the Academic Council at its meeting held on 5th May, 2018 **vide** item No. 4.45 and that in accordance therewith, the revised syllabus as per the (CBCS) for the T.Y.B.Com. (Banking and Insurance) (Sem. V & VI), has been brought into force with effect from the academic year 2018-19, accordingly. (The same is available on the University's website www.mu.ac.in).

MUMBAI – 400 032

12th June, 2018

To



(Dr. Dinesh Kamble)

I/c REGISTRAR

The Principals of the affiliated Colleges and Directors of the recognized Institutions in Commerce & Management Faculty. (Circular No. UG/334 of 2017-18 dated 9th January, 2018.)

A.C./4.45/05/05/2018

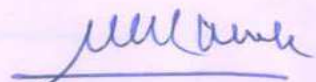
No. UG/ 7 -A of 2018

MUMBAI-400 032

12th June, 2018

Copy forwarded with Compliments for information to:-

- 1) The I/c Dean, Faculty of Commerce & Management,
- 2) The Director, Board of Examinations and Evaluation,
- 3) The Director, Board of Students Development,
- 4) The Professor-cum-Director, Institute of Distance and Open Learning (IDOL),
- 5) The Co-Ordinator, University Computerization Centre,



(Dr. Dinesh Kamble)

I/c REGISTRAR

University of Mumbai



**Revised Syllabus
and
Question Paper Pattern
of Courses of
B.Com. (Banking and Insurance)
Programme at
Third Year
*Semester V and VI***

**Under Choice Based Credit, Grading and
Semester System**

***(To be implemented from Academic Year 2018-2019)
Board of Studies-in-Banking & Finance***

B.Com. (Banking and Insurance) Programme

Under Choice Based Credit, Grading and Semester System

T.Y.B.Com. (Banking and Insurance)

(To be implemented from Academic Year 2018-2019)

No. of Courses	Semester V	Credits	No. of Courses	Semester VI	Credits
1	Elective Courses (EC)		1	Elective Courses (EC)	
1,2,3 &4	*Any four courses from the following list of the courses	12	1,2,3 &4	**Any four courses from the following list of the courses	12
2	Core Courses (CC)		2	Core Courses (CC)	
5	International Banking and Finance	04	5	Central Banking	04
3	Ability Enhancement Course(AEC)		3	Ability Enhancement Course (AEC)	
6	Research Methodology	04	6	Project Work In Banking & Insurance	04
Total Credits		20	Total Credits		20

✓ **Note:** Project work is considered as a special course involving application of knowledge in solving/analyzing/exploring a real life situation/ difficult problem. Project work would be of 04 credits each. A project work may be undertaken in any area of Elective Courses/ Study Area

*List of Elective Courses for Semester V (Any Four)		**List of Elective Courses for Semester VI (Any Four)	
01	Financial Reporting & Analysis(Corporate Banking & Insurance)	01	Security Analysis and Portfolio Management
02	Auditing - I	02	Auditing - II
03	Strategic Management	03	Human Resource Management
04	Financial Services Management	04	Turnaround Management
05	Business Ethics and Corporate Governance	05	International Business
06	Actuarial Analysis in Banking & Insurance	06	Marketing in Banking & Insurance
Note: Course selected in Semester V will continue in Semester VI			

B.Com. (Banking and Insurance) Programme
Under Choice Based Credit, Grading and Semester System
Course Structure

(To be implemented from Academic Year 2018-2019)

Semester V

No. of Courses	Semester V	Credits
1	<i>Elective Courses (EC)</i>	
1,2,3 & 4	*Any four courses from the following list of the courses	12
2	<i>Core Courses (CC)</i>	
5	International Banking and Finance	04
6	Research Methodology	04
Total Credits		20

<i>*List of Elective Courses for Semester V (Any Four)</i>	
01	Financial Reporting and Analysis(Corporate Banking & Insurance)
02	Auditing- I
03	Strategic Management
04	Financial Services Management
05	Business Ethics and Corporate Governance
06	Actuarial Analysis in Banking & Insurance

B.Com. (Banking and Insurance) Programme
Under Choice Based Credit, Grading and Semester System
Course Structure

(To be implemented from Academic Year 2018-2019)

Semester VI

No. of Courses	Semester VI	Credits
1	<i>Elective Courses (EC)</i>	
1,2,3 & 4	**Any four courses from the following list of the courses	12
2	<i>Core Courses (CC)</i>	
5	Central Banking	04
3	<i>Ability Enhancement Course</i>	
6	Project Work in Banking & Insurance	04
Total Credits		20

<i>*List of Elective Courses for Semester V (Any Four)</i>	
01	Security Analysis and Portfolio Management
02	Auditing - II
03	Human Resource Management
04	Turnaround Management
05	International Business
06	Marketing in Banking & Insurance

University of Mumbai



**B.Com. (Banking and Insurance)
Programme**

Guidelines for Project Work

at

**Third Year
Semester VI**

**Under Choice Based Credit, Grading and
Semester System**

(To be implemented from Academic Year 2018-2019)

Board of Studies-in-Banking and Finance

Introduction

Inclusion of project work in the course curriculum of the B.Com. (Banking and Insurance) programme is one of the ambitious aspects in the programme structure. The main objective of inclusion of project work is to inculcate the element of research analyse and scientific temperament challenging the potential of learner as regards to his/ her eager to enquire and ability to interpret particular aspect of the study. It is expected that the guiding teacher should undertake the counselling sessions and make the awareness among the learners about the methodology of formulation, preparation and evaluation pattern of the project work.

- There are two modes of preparation of project work
 1. Project work based on research methodology in the study area
 2. Project work based on internship in the study area

Guidelines for preparation of Project Work

1. General guidelines for preparation of project work based on Research Methodology

- The project topic may be undertaken in any area of Elective Courses.
- Each of the learner has to undertake a Project individually under the supervision of a teacher-guide.
- The learner shall decide the topic and title which should be specific, clear and with definite scope in consultation with the teacher-guide concerned.
- University/college shall allot a guiding teacher for guidance to the students based on her / his specialization.
- The project report shall be prepared as per the broad guidelines given below:
 - Font type: Times New Roman
 - Font size: 12-For content, 14-for Title
 - Line Space : 1.5-for content and 1-for in table work
 - Paper Size: A4
 - Margin : in Left-1.5, Up-Down-Right-1
 - The Project Report shall be bounded.
 - The project report should be 80 to 100 pages

Format

1st page (Main Page)

Title of the problem of the Project

A Project Submitted to
University of Mumbai for partial completion of the degree of
Bachelor in Commerce (Banking and Insurance)
Under the Faculty of Commerce

By

Name of the Learner

Under the Guidance of

Name of the Guiding Teacher

Name and address of the College

Month and Year

2nd Page

This page to be repeated on 2nd page (i.e. inside after main page)

On separate page

Index

Chapter No. 1 (sub point 1.1, 1.1.1, And so on)	Title of the Chapter	Page No.
Chapter No. 2	Title of the Chapter	
Chapter No. 3	Title of the Chapter	
Chapter No. 4	Title of the Chapter	
Chapter No. 5	Title of the Chapter	

List of tables, if any, with page numbers.

List of Graphs, if any, with page numbers.

List of Appendix, if any, with page numbers.

Abbreviations used:

Structure to be followed to maintain the uniformity in formulation and presentation of Project Work

(Model Structure of the Project Work)

- **Chapter No. 1: Introduction**

In this chapter Selection and relevance of the problem, historical background of the problem, brief profile of the study area, definition/s of related aspects, characteristics, different concepts pertaining to the problem etc can be incorporated by the learner.

- **Chapter No. 2: Research Methodology**

This chapter will include Objectives, Hypothesis, Scope of the study, limitations of the study, significance of the study, Selection of the problem, Sample size, Data collection, Tabulation of data, Techniques and tools to be used, etc can be incorporated by the learner.

- **Chapter No. 3: Literature Review**

This chapter will provide information about studies done on the respective issue. This would specify how the study undertaken is relevant and contribute for value addition in information/ knowledge/ application of study area which ultimately helps the learner to undertake further study on same issue.

- **Chapter No. 4: Data Analysis, Interpretation and Presentation**

This chapter is the core part of the study. The analysis pertaining to collected data will be done by the learner. The application of selected tools or techniques will be used to arrive at findings. In this, table of information's, presentation of graphs etc. can be provided with interpretation by the learner.

- **Chapter No. 5: Conclusions and Suggestions**

In this chapter of project work, findings of work will be covered and suggestion will be enlisted to validate the objectives and hypotheses.

Note: If required more chapters of data analysis can be added.

- **Bibliography**
- **Appendix**

On separate page

Name and address of the college

Certificate

This is to certify that Ms/Mr _____ has worked and duly completed her/his Project Work for the degree of Bachelor in Commerce (Banking and Insurance) under the Faculty of Commerce in the subject of _____ and her/his project is entitled, “ _____ *Title of the Project* _____ ” under my supervision.

I further certify that the entire work has been done by the learner under my guidance and that no part of it has been submitted previously for any Degree or Diploma of any University.

It is her/ his own work and facts reported by her/his personal findings and investigations.



Name and Signature of
Guiding Teacher

Date of submission:

On separate page

Declaration by learner

I the undersigned Miss / Mr. _____ *Name of the learner* _____ here by,
declare that the work embodied in this project work titled “ _____
_____ *Title of the Project* _____ ”,
forms my own contribution to the research work carried out under the guidance of
_____ *Name of the guiding teacher* _____ is a result of my own research work and has
not been previously submitted to any other University for any other Degree/ Diploma
to this or any other University.

Wherever reference has been made to previous works of others, it has been clearly
indicated as such and included in the bibliography.

I, here by further declare that all information of this document has been obtained and
presented in accordance with academic rules and ethical conduct.

Name and Signature of the learner

Certified by

Name and signature of the Guiding Teacher

On separate page

Acknowledgment

(Model structure of the acknowledgement)

To list who all have helped me is difficult because they are so numerous and the depth is so enormous.

I would like to acknowledge the following as being idealistic channels and fresh dimensions in the completion of this project.

I take this opportunity to thank the **University of Mumbai** for giving me chance to do this project.

I would like to thank my **Principal**, _____ for providing the necessary facilities required for completion of this project.

I take this opportunity to thank our **Coordinator** _____, for her moral support and guidance.

I would also like to express my sincere gratitude towards my project guide _____ whose guidance and care made the project successful.

I would like to thank my **College Library**, for having provided various reference books and magazines related to my project.

Lastly, I would like to thank each and every person who directly or indirectly helped me in the completion of the project especially **myParents and Peers** who supported me throughout my project.

2. Guidelines for Internship based project work

- Minimum 20 days/ 100 hours of Internship with an Organisation/ NGO/ Charitable Organisation/ Private firm.
- The theme of the internship should be based on any study area of the elective courses
- Experience Certificate is Mandatory
- A project report has to be brief in content and must include the following aspects:
 - **Executive Summary:**
A bird's eye view of your entire presentation has to be precisely offered under this category.
 - **Introduction on the Company:**
A Concise representation of company/ organization defining its scope, products/ services and its SWOT analysis.
 - **Statement and Objectives:**
The mission and vision of the organization need to be stated enshrining its broad strategies.
 - **Your Role in the Organisation during the internship:**
The key aspects handled, the department under which you were deployed and brief summary report duly acknowledged by the reporting head.
 - **Challenges:**
The challenges confronted while churning out theoretical knowledge into practical world.
 - **Conclusion:**
A brief overview of your experience and suggestions to bridge the gap between theory and practice.
- The project report based on internship shall be prepared as per the broad guidelines given below:
 - Font type: Times New Roman
 - Font size: 12-For content, 14-for Title
 - Line Space : 1.5-for content and 1-for in table work
 - Paper Size: A4
 - Margin : in Left-1.5, Up-Down-Right-1
 - The Project Report shall be bounded.
 - The project report should be of minimum 50 pages

Evaluation pattern of the project work

The Project Report shall be evaluated in two stages viz.	
• Evaluation of Project Report (Bound Copy)	60 Marks
▪ Introduction and other areas covered	20 Marks
▪ Research Methodology, Presentation, Analysis and interpretation of data	30 Marks
▪ Conclusion & Recommendations	10 Marks
• Conduct of Viva-voce	40 Marks
▪ In the course of Viva-voce, the questions may be asked such as importance / relevance of the study, objective of the study, methodology of the study/ mode of Enquiry (question responses)	10 Marks
▪ Ability to explain the analysis, findings, concluding observations, recommendation, limitations of the Study	20 Marks
▪ Overall Impression (including Communication Skill)	10 Marks

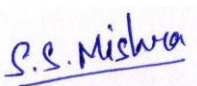
Note:


- *The guiding teacher along with the external evaluator appointed by the University/ College for the evaluation of project shall conduct the viva-voce examination as per the evaluation pattern*

Passing Standard

- Minimum of Grade E in the project component
- In case of failing in the project work, the same project can be revised for ATKT examination.
- Absence of student for viva voce: If any student fails to appear for the viva voce on the date and time fixed by the department such student shall appear for the viva voce on the date and time fixed by the Department, such student shall appear for the viva voce only along with students of the next batch.

Sonopant Dandekar Arts. V.S.Apte Commerce and M.H.Mehta Science College, Palghar			
T.Y.BBI PROJECT SUBMISSION SEM VI 2022-23			
Sr. No	Name of the Student	Area of Study	Project Title
1	DASH DEEPIKA TUMANATH	Banking & Insurance	Comparative study between private sector and public sector bank
2	DUBEY SURAJ KANIKBHAWAN	Banking & Insurance	A Study of Trends of Gold Loan in Public Sector bank & NBFC
3	GHUSALE ROSHNI BALU	Banking & Insurance	A study on prospectus and challenges of mobile banking in India
4	JAIN MEET ASHISH	Banking & Insurance	An inside into the Indian money market through HDFC bank : A case study
5	HRITHIK RANJEET JHA	Banking & Insurance	A study on AI, Indian banking sector
6	MACHHI VRUSHABH JAGDISH	Banking & Insurance	Internet Banking system
7	MISHRA CHETANA RAMESH	Banking & Insurance	A study on impact of electronic banking on customers
8	MOURYA VIJAY SURENDRA	Banking & Insurance	A detailed study on the function of banking sector
9	PAL BEAUTI RAMDHANI	Banking & Insurance	A study on housing scheme of public loans
10	YOGESH PAREEK	Banking & Insurance	Detailed study on fraud and scams in banking industry
11	RAJPUROHIT KHUSHBOO	Banking & Insurance	Non-banking financial services
12	SHINDE KOMAL GANESH	Banking & Insurance	A study of cash management in SBI
13	SINGH PALLAVI SHIVKARAN	Banking & Insurance	A critical study on investment banking
14	SINGH RAHUL KRISHNA	Banking & Insurance	A study on different loan service provided by Bajaj finance
15	YADAV MUKESH LALLU	Banking & Insurance	Study procedures of home loan process of PNB and ICICI
16	YADAV PRIYANKA AMALA	Banking & Insurance	Comparison study on the education loan provided by the SBI bank and ICICI bank


(Dr. Shreya Mishra)
HOD
Department of BBI


(Dr. Kiran J. Save)
Principal
PRINCIPAL
Sonopant Dandekar Arts College,
V.S. Apte Commerce College &
M.H. Mehta Science College
PALGHAR (W.R.)
Dist. Palghar, Pin-401404

**Sonopant Dandekar Arts, V.S. Apte Commerce and M.H.
Mehta Science College, Palghar**
T.Y.BBI External Viva-voce Examination
Attendance Report

Date - 13th April, 2023

Time - 8 am to 10 am

Venue - Classroom No. BMS 16

Sr.No.	Name of the Student	Signature
1	DASH DEEPIKA TUMANATH	Deepika
2	DUBEY SURAJ KANIKBHAWAN	Suraj
3	GHUSALE ROSHNI BALU	Roshni
4	JAIN MEET ASHISH	Meet
5	HRITHIK RANJEET JHA	HRITHIK
6	MACHHI VRUSHABH JAGDISH	Vrushabh
7	MISHRA CHETANA RAMESH	Chetana
8	MOURYA VIJAY SURENDRA	Mourya
9	PAL BEAUTI RAMDHANI	Beauti
10	YOGESH PAREEK	Yogesh
11	RAJPUROHIT KHUSHBOO	Rajpurohit
12	SHINDE KOMAL GANESH	Komal
13	SINGH PALLAVI SHIVKARAN	Pallavi
14	SINGH RAHUL KRISHNA	Rahul
15	YADAV MUKESH LALLU	Mukesh
16	YADAV PRIYANKA AMALA	Priyanka

Rajya
13/4/23
Rajya Poojinder Shetty
Name and Signature of External Examiner

PROJECT REPORT

ON

“Detailed study on fraud & scams in Banking Industry”

SUBMITTED TO THE UNIVERSITY OF MUMBAI IN THE PARTIAL
FULFILMENT OF THE DEGREE BACHELOR OF MANAGEMENT
STUDIES.

SUBMITTED BY:

YOGESH PAREEK

T.Y.BBI

ACADEMIC YEAR: 2022-23

PROJECT GUIDE:

Ms. KRUTIKA D. PATEL

M.COM(Accountancy)

SUBMITTED TO:

UNIVERSITY OF MUMBAI



SONOPANT DANDEKAR R.H.SAVE INSTITUTE OF MANAGEMENT,
PALGHAR DIST: PALGHAR PIN: 401404 UNIVERSITY OF MUMBAI ARTS,
V.S.APTE COMMERCE AND M.H.MEHTA COLLEGE,

DECLARATION

I, **YOGESH PAREEK**, A STUDENT OF SONOPANT DANDEKAR ARTS, V.S.APTE COMMERCE AND M.H.MEHTA SCIENCE COLLEGE, R.H.SAVE INSTITUTE OF MANAGEMENT, PALGHAR DIST:- PALGHAR, PIN:- 401 404 STUDYING IN T.Y.BBI HEREBY DECLARE THAT I HAVE COMPLETED THIS PROJECT ON “**Detailed study on fraud & scams in Banking sector**” DURING THE ACADEMIC YEAR 2022-23 THE INFORMATION SUBMITTED IS TRUE AND ORIGINAL TO THE BEST OF MY KNOWLEDGE.

DATE: 14th April 2023


SIGNATURE OF STUDENT

YOGESH PAREEK

PLACE: PALGHAR

CERTIFICATE

I, Ms. KRUTIKA D. PATEL, HEREBY CERTIFY THAT **YOGESH PAREEK** OF SONOPANT DANDEKAR ARTS, V.S.APTE COMMERCE AND M.H.MEHTA SCIENCE COLLEGE, R.H.SAVE INSTITUTE OF MANAGEMENT, PALGHAR DIST:- PALGHAR, PIN:- 401 404 OF T.Y.BBI HAS COMPLETED **HIS** PROJECT ON “**DETAILED STUDY ON FRAUD & SCAMS IN BANKING INDUSTRY**” DURING THE ACADEMIC YEAR 2022-23. THE INFORMATION SUBMITTED IS TRUE AND ORIGINAL TO THE BEST OF MY KNOWLEDGE.



Ms. KRUTIKA D. PATEL



SIGNATURE OF THE
PRINCIPAL OF COLLEGE

SIGNATURE OF PROJECT

GUIDE



SIGNATURE OF CO-ORDINATOR



SIGNATURE OF
EXTERNAL EXAMINER

INDEX

Sr.No	Topic	Page No.
1	Introduction	1
1.1	Definition of fraud & Scams in Banking Industry	4
1.2	Types & Classification of Bank Frauds	6
1.3	Classification of fraud by RBI	8
1.4	Types of fraud Reported in FY 20-21	13
1.5	Fraud Reported over the years	14
1.6	Historical Perspective	16
1.7	Major Reasons for Bank Fraud	17
1.8	Who can commit bank fraud	18
1.9	How Fraud & Scams have Overhelm India	20
1.10	Causes of Fraud & Scams in Banking Sector	21
1.11	What We learn from this Causes	23
1.12	Impact on banking Sector	24
1.13	Impact on Customers	26
1.14	Detention & Prevention Technique	27
1.15	Regulatory Framework	29
1.16	Future Outlook	33
1.17	International Perspective	34
1.18	What Is Contributng to Rise in Fraud	35
2	Data Analysis	36
3	Interview Based findings	40
4	Data Meaning	60
5	Conclusion	72
6	Recommendations	73
7	Bibliography	79

ACKNOWLEDGEMENT

If words are considered as a symbol of approval and token of appreciation then let the words play the heralding role expressing my gratitude. My successful completion of this project report involved more than just my desire to earn a valued degree working on this project has presented me with many insights and challenges.

I would like to thank the university of Mumbai for introducing bachelor of management studies course, thereby giving its student a platform to abreast with changing business scenario, with the help of theory as a base and practical as a solution- I am also thankful to the management of S.D.S.M College of PALGHAR for making all the facilities available and espousing the cause of the research. I would like to thank our honorable principal **Dr.Kiran Save**

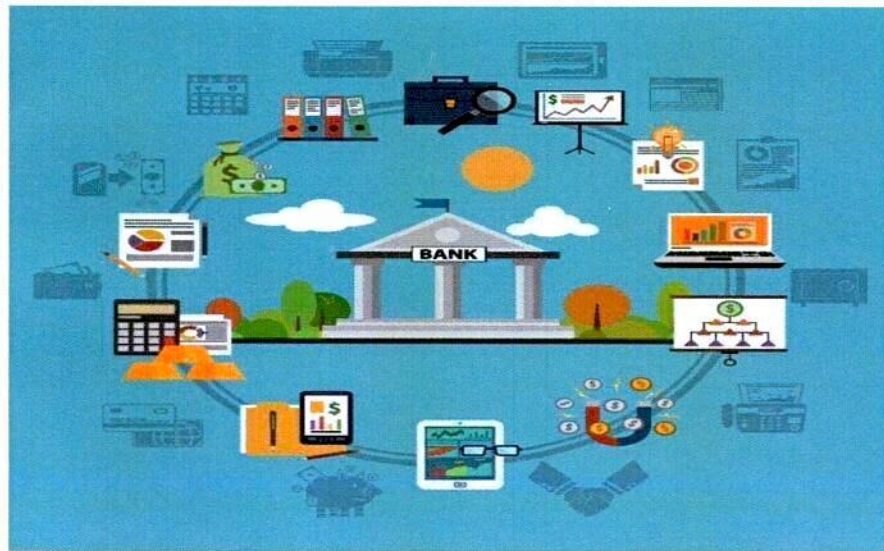
I would like to express my earnest gratitude to **Prof. KRUTIKA PATEL** for her superlative guidance and unflinching support throughout the project work. No development would have been feasible had it not been for their excellent supervision, constant encouragement and careful perusal, in completion of the project successfully.

Last but not the least; I would like to thank my parents & teachers for giving the best education and friends for their support and feelings without which this project would have not been possible. Many others without whose invaluable help and expert advice this project would not have been the same ought to be cited.

With the completion of my project entitled “ DETAILED STUDY ABOUT FRAUD & SCAMS IN BANKING INDUSTRY”

- **YOGESH PAREEK**

DETAILED STUDY ABOUT FRAUD & SCAMS IN BANKING INDUSTRY



EXECUTIVE SUMMARY

This project examines the problem of fraud and scams in the banking sector, with a focus on the Indian context. The project provides an overview of the historical perspective of fraud in banking and identifies the key causes of fraud and scams in the industry, including factors such as weak internal controls, employee fraud, and cybercrime.

The project also analyzes the impact of fraud and scams on the banking sector, including financial losses, reputational damage, and loss of customer trust. To address this problem, the project outlines detection and prevention techniques such as employee training, fraud risk assessments, and the use of technology solutions.

Additionally, the project explores the regulatory framework surrounding fraud and scams in the banking sector and discusses the role of regulators in preventing and detecting fraud. Finally, the project presents case studies of real-world fraud incidents and offers a future outlook for the industry, emphasizing the importance of a multi-faceted approach to combat fraud and scams in the banking sector.

The study intends to fulfil the following two objectives – a) to understand and analyse underlying causes contributing to increasing trend in frauds committed in Indian banking sector; and b) to suggest appropriate and suitable measures that can help the system in addressing these issues

Introduction and Issues

In recent years, instances of financial fraud have regularly been reported in India. Although banking frauds in India have often been treated as cost of doing business, post liberalisation the frequency, complexity and cost of banking frauds have increased manifold resulting in a very serious cause of concern for regulators, such as the Reserve Bank of India (RBI). RBI, the regulator of banks in India, defines fraud as “A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank”

In the recent years, public sector banks (PSBs) in India have lost a total of Rs. 1.96 lakh crore, on account of various banking frauds. With various measures initiated by the RBI, numbers of banking fraud cases have declined, but amount of money lost has increased in these years. Prima facie, an initial investigation in these cases has revealed involvement of not only mid-level employees, but also of the senior most management as was reflected in the case of Syndicate Bank and Indian Bank. This raises serious concern over the effectiveness of corporate governance at the highest Rank of these banks. In addition, there has been a rising trend of non-performing assets (NPAs), especially for the PSBs, thereby severely impacting their profitability. Several causes have been attributed to risky NPAs, including global and domestic slowdown, but there is some evidence of a relationship between frauds and NPAs as well.

The robustness of a country’s banking and financial system helps determine its production and consumption of goods and services.

It is a direct indicator of the well-being and living standards of its citizens. Therefore, if the banking system is plagued with high levels of NPAs then it is a cause of worry, because it reflects financial distress of borrower clients, or inefficiencies in transmission mechanisms. Indian economy suffers to a great extent from these problems, and this served as the prime motivation for the authors to carry out this detailed study of frauds in the Indian banking system and examining frauds from different angles.

This study takes into consideration, different aspects of Indian banking sector. Finally, an attempt has been made to give possible recommendations that can help mitigate these problems.

The rest of the paper is organized into three major sections. Section 2 is a review of existing literature on the global and domestic banking sector. It talks of the evolution of the regulatory landscape governing the banking system as well as a discussion of existing literature on the issues of NPAs in banks and incidence of banking fraud. Section 3 provides a detailed analysis of banking frauds in India. It broadly covers two categories of studies carried out – secondary research from literature and case studies and primary research from interviews spanning across all players involved in reporting of financial misconduct. Section 4 provides a detailed set of recommendations for prevention and early detection of frauds in banking system.

The study intends to fulfil the following two objectives –

- A) To understand and analyse underlying causes contributing to increasing trend in frauds committed in Indian banking sector
- B) To suggest appropriate and suitable measures that can help the system in addressing these issues.

To maintain uniformity in fraud reporting, frauds have been classified by RBI based on their types and provisions of the Indian penal code, and reporting guidelines have been set for those according to RBI (2014 and 2015).

Impartial policy guidelines and whistle-blower policy are vital to empower employees to handle frauds. RBI also issued a circular and introduced the concept of Red flagged account (RFA), based on the presence of early warning signals (EWS), into the current framework, for early detection and prevention of frauds. Gandhi (2014) discussed the prime causes of growing NPAs and recognised the absence of robust credit appraisal system, inefficient supervision post credit disbursal, and ineffective recovery mechanism as key barriers addressing those aspects. Gandhi (2015) stressed on the basic principles that can go a long way in preventing fraud, namely the principles of knowing the customer and employees as well as partners. He also pointed out the significance of a robust appraisal mechanism and continuous monitoring.

Reports suggests that financial innovations have led to higher aggregate borrowings, which has resulted in higher defaults.

DEFINITION OF FRAUD & SCAMS IN BANKING SECTOR

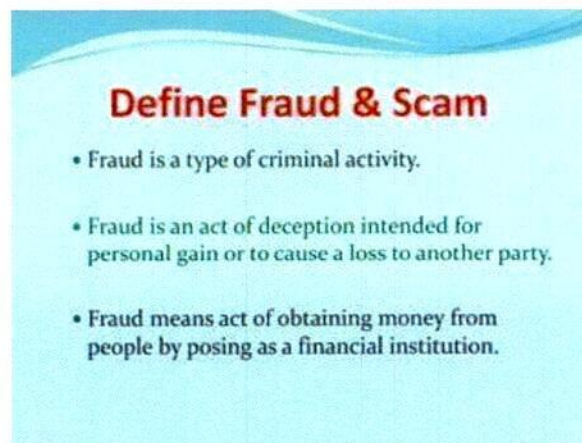
Fraud is generally defined as a deliberate deception to secure an unfair or unlawful gain, usually for personal or financial gain. In the banking sector, fraud can take many forms, including embezzlement, identity theft, forgery, and money laundering.

Scams, on the other hand, are typically fraudulent schemes designed to trick people into giving away their money or personal information. Scams can take many forms, such as phishing emails, fake investment opportunities, and fraudulent loan offers.

In the banking sector, scams often involve social engineering tactics to trick individuals into divulging sensitive information or giving access to their accounts. For example, a scammer may pose as a bank representative and ask for personal information, or send a fake email asking for login credentials.

Both fraud and scams can have serious consequences for individuals and the banking sector as a whole, including financial losses, damage to reputation, and legal and regulatory consequences.

It is essential for banks and their customers to remain vigilant and take proactive measures to prevent and detect fraud and scams.



In all bank fraud cases, the sections: under IPC covering cheating, concealment, counterfeiting, misappropriation, breach of trust, criminal conspiracy, etc are only being invoked at present. The recourse to these sections is because there was no proper section in IPC defining bank frauds and punishments therefor. Even now there is no proper definition to bank frauds in the legal sense. However, wellknown Study Group has attempted the following definition

A Bank Fraud is a deliberate act of omission or commission by any person carried out in the course of a banking transaction or in the books of account maintained manually or under computer systems in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank.

By modification, the following definition for bank frauds is attempted

A Bank Fraud means and includes any of the following acts committed by any person with his connivance, or by his agent including a banker with an Intention to cheat or actually cheat or conceal or falsify or forge documents, accounts or indulge in misappropriation which results in wrongful gain to any person with or without monetary loss in the course of banking transactions.

TYPES AND CLASSIFICATION OF BANK FRAUDS

Any transaction having the following features can be categorized as a bank fraud

- ① Shortage of cash
- ② Fraudulent encashment of drafts/cheques/travelers cheques, dividend warrants, etc
- ③ Fraudulent endorsement of cheques, drafts, bills etc with an intention of conversion to Encash the same
- ④ Opening bogus bank accounts in the name of non-existing persons
- ⑤ Collecting fake instruments with or without connivance of bank staff
- ⑥ Siphoning off funds through the fake telegraphic/mail transfers, unauthorized debits of impersonal accounts and/or concealment of any unauthorized transaction by manipulating entries in the books of accounts
- ⑦ Creation of fixed deposits, credit balances and issuance of drafts, pay orders, stock invest, etc without consideration
- ⑧ Sudden disappearance of stocks as compared to the figures shown in the previous statement.
- ⑨ Issuance of letters of credit, bank guarantees, etc without recording liability in the books of accounts
- ⑩ Misuse of computer code and breach of security of computer systems

FRAUD CASES

Banks	2018-19		2019-20		Apr-Jun 2020	
	No of frauds	Amount involved	No of frauds	Amount involved	No of frauds	Amount involved
Public sector banks	3,568	63,283	4,413	1,48,400	745	19,958
Private sector banks	2,286	6,742	3,066	34,211	664	8,009
Foreign banks	762	955	1,026	972	127	328
Financial institutions	28	553	15	2,048	3	546
Small finance banks	115	8	147	11	16	2
Payments banks	39	2	38	2	3	0
Local area banks	1	0.02	2	0.43	0	0
Total	6,799	71,543	8,707	1,85,644	1,558	28,843

This figure shows the fraud cases reported by different types of banks

Both public sector and private banks in India have faced fraud cases in recent years. While there have been reports of major fraud cases involving public sector banks such as Punjab National Bank, Bank of Baroda, and Canara Bank, there have also been instances of fraud in private banks such as ICICI Bank, HDFC Bank, and Axis Bank. **It is important to note that fraud can occur in any bank, regardless of its ownership or size.**

Classification of frauds by RBI

In order to have uniformity in reporting cases of frauds, the question of classification of bank frauds on the basis of the provisions of the IPC has been considered and frauds have been classified as under

- ① Misappropriation and criminal breach of trust
- ② Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property '
- ③ Unauthorized credit facilities extended for reward or for illegal gratification
- ④ Negligence and cash shortages
- ⑤ Cheating and forgery
- ⑥ Irregularities in foreign exchange transactions
- ⑦ Any other type of fraud not coming under the specific heads as above

Cases of 'negligence and cash shortages' referred to in item under "Negligence and cash shortages above are to be reported as frauds if the intention to cheat/defraud is suspected/proved.

Cases of theft and burglary should not be reported as frauds.

All cases of theft, burglary, dacoity and robbery may be reported separately.

Computer Frauds in Banks

Computer frauds are those involving embezzlements or defalcations achieved by tampering with computer data, record or programme, etc.

Computer crimes are those committed with the help of a computer like theft, forgery, counterfeiting, etc

Computer crimes are committed mainly for gaining money. But other motives can also be enumerated like

- (A) Personal Revenge
- (B) Blackmail
- (C) Ego
- (D) Mental aberrations
- (E) Mischief
- (F) Playfulness

All stages of computer operations are susceptible to criminal activity either as the target of the crime or as the instrument of the crime or both. Input operations, data processing, output operations and communications are being utilized for illicit purposes. With introduction of computers in the banks in a big way they have also in a way, become susceptible to computer related crimes.

The most common types are

Fraud by computer manipulation: Intangible assets represented in data format such as money on deposits or hours of work are the most common targets of computer related fraud. Modern banking business is quickly replacing cash with deposits transacted on computer systems, creating an enormous potential for computer abuse. Credit card information, as well as personal and financial information about credit card clients, has been the most frequently targeted area.

The sale of this information to counterfeiters of credit cards and travel document fraudsters has proven to be extremely lucrative. Assets represented in data format often have a considerably higher value than traditionally targeted economic assets resulting in potentially greater economic loss. Improved remote access to databases in the banks allows the criminal the opportunity to commit various types of frauds without ever entering its premises.

Computer fraud by input manipulation is easy to perpetrate and difficult to detect. It is called "data diddling".

It does not require any sophisticated computer knowledge. It can be committed by anyone having access to normal data processing functions. The incidence of allowing access to computers by all and sundry in the banks is a high-risk prone area.

Programme Manipulation: It is very difficult to discover and is frequently not recognized and requires the perpetrator to have computer-specific knowledge. It involves changing existing programmes in the computer systems or inserting new programmes or routines. A common method used by persons with specialized knowledge of computer programming is called the Trojan Horse, in which computer instructions are covertly hidden in a computer programme so that it will perform an unauthorized function concurrent with its normal function.

A Trojan Horse can be programmed to self-destruct, thereby, leaving no evidence of its existence except the damage that it had caused. Remote access capabilities today also allow the criminal to easily run modified routines concurrently with legitimate programmes. All the computerization of the banks has been programme-specific and is heavily routinized making their computers vulnerable to misuse.

Output Manipulation: It is effected by targeting the output of the computer system. An example is a cash dispenser fraud, achieved by falsifying Instructions to the computer in the input stage. Traditionally, such fraud involved the use of stolen bankcards. However, specialized computer hardware and software is now being widely used to encode falsified electronic information of the magnetic strips of bankcards and credit cards.

There is a particular species of fraud conducted by computer manipulation that takes advantage of the automatic repetitions of computer processes.

Such manipulation is characteristic of a specialized “salami technique”, in which nearly unnoticeable “thin slices” of financial transactions are repeatedly stolen and transferred to another account.

Computer Forgery: A computer forgery is committed when the data, which is stored in a computerized form, is deliberately altered. Computer systems are the target of this criminal activity. Computers, however, can also be used as instruments to commit forgery. They have created a new library of tools with which one can forge the documents used in commerce very easily. A new generation of fraudulent alteration or counterfeiting emerged when computerized colour laser copiers became available.

These copiers are capable of high-resolution copying, modification of documents and even the creation of false documents without even having the need of possessing an original. They produce documents whose quality is indistinguishable from that of the authentic documents. Any document including the security forms like cheques, drafts, etc. can be very easily created with this kind of processes available at present.

Damage to or modifications of computer data or programs: This category of criminal activity involves either direct or covert unauthorized access to a computer system by the introduction of new programmes known as viruses, worms or logic bombs. These activities are also called computer sabotage and involve unauthorized modification or damage of legitimate computer data or programmes. A virus is a series of programme codes, which has the ability to attach itself to legitimate programmes and propagate itself to other computer programmes. This can potentially damage the data available in the computer systems. A worm is one, which replicates itself by bringing the systems to a stage of complete crash. A logic bomb is like a time bomb, which can be detonated at the will of the perpetrator.

Unauthorized access to computer systems and service: Unauthorized access is often accomplished from a remote location along telecommunication network. Password is often mischaracterized as a protective device against unauthorized access. But this can be easily circumvented if a hacker is able to discover a password allowing access.

Password protection can also be bypassed successfully by utilizing password-cracking routines. The third method commonly used is a "trapdoor" method in which unauthorized access is achieved through access points or trapdoors created for legitimate purposes such as maintenance of the system.

Unauthorized Reproduction of legally protected computer programme: The unauthorized reproduction of computer programmes can mean a substantial economic loss to the legitimate owners. The problem has reached transnational dimensions with the trafficking of these unauthorized reproductions over modern telecommunication networks,

Unauthorized Electronic Fund Transfers: The most important type is the committing of a fraud by manipulation of input, output or throughput of a computer based system. Output manipulation is achieved by affecting the output of the system such as the one entailing the use of stolen or falsified cards in ATM Machines.

Crimes in electronic fund transfer like ATMs, Credit Cards, Debit Cards, etc include

- (A) Diversion of the money from the customer to a fraudulent payee
- (B) Credit cards are copied and data misused
- (C) Credit cards are stolen
- (D) Lost credit cards are used by unauthorized persons
- (E) White cards are used in place of original cards
- (F) Wires are tapped and necessary data stolen to operate ATM accounts
- (G) Withdrawals and deposits manipulation (h) Fraudulent telemarketing.

TYPES OF FRAUD REPORTED IN FY 20-21

According to a report by the Reserve Bank of India (RBI), the types of frauds reported in the Indian banking system during the fiscal year 2020-21 are:

Loan fraud	32.6%
Card/ATM fraud	22.1%
Internet banking and phishing fraud	16.9%
Off-balance sheet fraud	8.6%
Fraudulent transfers	6.9%
Deposit-related fraud	6.3%
Cash-related fraud	3.8%
Other types of fraud	3.0%

There are a few reasons why loan fraud is one of the most common types of bank fraud. One reason is that loans typically involve large amounts of money, making them attractive targets for fraudsters. Additionally, loans often require extensive documentation and verification, which can create opportunities for fraudsters to provide false information or manipulate the process.

Another factor is that loan fraud can take many forms, including falsifying income or employment information, submitting fraudulent loan applications, or misrepresenting collateral. In some cases, fraudsters may even create fake companies or use stolen identities to obtain loans.

Furthermore, loan fraud can be difficult to detect and prosecute, as it often involves complex financial transactions and can be carried out over a long period of time. This can make it challenging for banks and law enforcement agencies to identify and track down the perpetrators.

Overall, loan fraud is a serious issue that can have significant consequences for both the financial system and individual consumers. It requires ongoing vigilance and effective measures to prevent and combat.

FRAUD REPORTED OVER THE YEARS

According to the Reserve Bank of India's Annual Report for 2020-21, the number and value of fraud cases reported in the Indian banking system over the last few years are as follows:

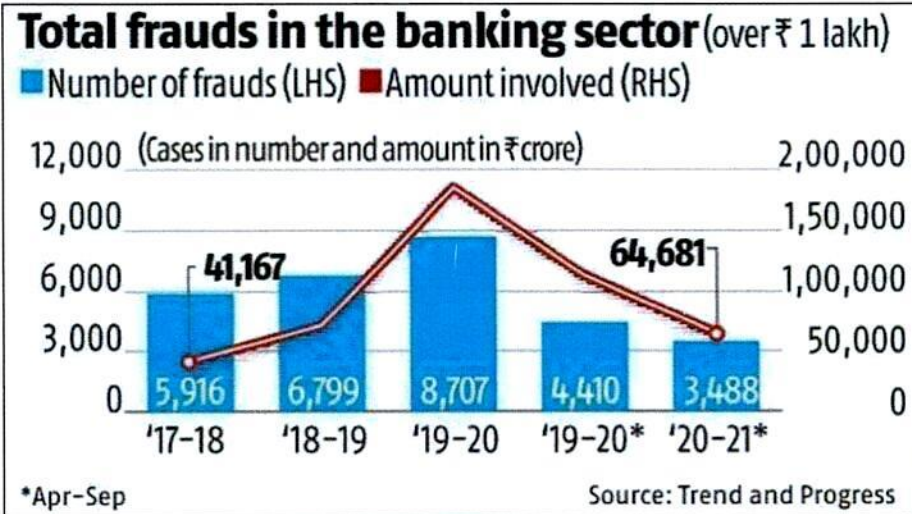
Financial Year	Number of Fraud Cases Reported	Amount Involved (in Rs. crore)
2016-17	5076	23,933
2017-18	5916	41,167
2018-19	6799	71,542
2019-20	4410	35,636
2020-21	3488	1,71,349

The data shows a significant increase in both the number and value of fraud cases reported in the Indian banking system over the past few years, **with the financial year 2020-21 witnessing the highest number of cases and the highest amount involved.**

It is important to note that these numbers are subject to change and may vary depending on the source and the time of reporting. Additionally, the actual numbers may be higher as some cases may go unreported or undetected.

From the above analysis it can be concluded that

- ① Liberalization of the economy has prodded increase in bank frauds
- ② A comprehensive policy for preventing frauds could not be developed
- ③ The regulatory bodies have either showed indifferent attitude or have summarily failed in their regulatory duties
- ④ In the search for more and more new customers the banks both in the public and private sector have thrown their caution to winds



This chart clearly shows that how fraud & scam has increased in banking sector over the years. The increase in bank fraud cases in India over the years can be attributed to various factors, such as technological advancements, inadequate regulations and oversight, and complexity of financial transactions.

HISTORICAL PERSPECTIVE REGARDING FRAUD & SCAMS IN BANKING SECTOR OF INDIA

Fraud and scams have also been present in the banking industry of India for a long time. One of the earliest recorded cases was the Mundhra Scandal in the 1950s, where the owner of a private company, Haridas Mundhra, colluded with several high-ranking government officials and bank executives to defraud Indian banks and investors.

In the 1990s, the Indian banking industry witnessed a series of high-profile scams, including the securities scam of 1992, which involved the manipulation of stock prices and resulted in significant losses for investors, and the Harshad Mehta Scam of 1992, where stockbroker Harshad Mehta used a loophole in the banking system to defraud banks and manipulate the stock market. In recent years, the Indian banking industry has been hit by several major frauds, such as the Nirav Modi PNB fraud case in 2018, which involved the fraudulent issuance of letters of undertaking (LOUs) by employees of the Punjab National Bank to companies associated with Nirav Modi, resulting in a loss of over \$2 billion.

The Indian banking industry has also been impacted by scams such as online banking fraud, ATM skimming, and phishing attacks. The increasing use of technology in the banking industry has made it easier for fraudsters to carry out their activities, and banks have had to constantly update their security measures to prevent such incidents.

MAJOR REASONS FOR BANK FRAUDS

Insider fraud: Bank frauds can occur when employees or insiders of a bank engage in fraudulent activities such as embezzlement, misappropriation of funds, or manipulation of accounting records.

Cyber fraud: With the increasing use of technology in banking, cyber fraud has become a significant threat. It includes phishing, hacking, and other forms of cybercrime that aim to steal personal or financial information.

Money laundering: Banks can be used as a tool for money laundering, where individuals or organizations use the bank's services to disguise the origins of illegally obtained funds.

Collusion: Bank frauds can also occur due to collusion between bank employees and outsiders such as customers, vendors, or other third parties.

Ponzi schemes: Ponzi schemes involve using funds from new investors to pay returns to earlier investors. Banks can unknowingly become part of a Ponzi scheme when they allow fraudulent operators to open accounts or process transactions.

Loan fraud: Banks can be victims of loan fraud when borrowers provide false information to obtain loans or misuse loan funds.

Identity theft: Bank frauds can occur when someone steals another person's identity to obtain access to their bank accounts or credit card information.

These are some of the major reasons and causes of bank frauds, and banks must implement robust security measures and policies to prevent them.

WHO CAN COMMIT BANK FRAUDS

To say that human beings only can commit frauds is evidently a hackneyed truism. It is often mistaken that some human beings are by nature fraudulent, dishonest and criminal and only such people can commit frauds. But it is not true that only some branded people commit frauds. Many factors actively contribute to make a normal person a fraudster. All these factors are often very clearly related to morality, religion, social circumstances, and intense needs of each fraudster.

Anyone can commit fraud, including bank employees, customers, and third-party actors. Bank employees who have access to sensitive information and transaction records are often in a position to commit fraud. Customers may also attempt to commit fraud, for example, by providing false information on loan applications or engaging in unauthorized transactions. Third-party actors, such as hackers and fraudsters, may attempt to steal funds or access confidential information through cyber attacks or social engineering tactics. It is important for banks to have robust fraud prevention measures in place to detect and prevent fraudulent activities.

What makes a man dishonest is solely dependent on factors unique only to that person. However, according to section 24 of IPC, whoever does anything with the intention of causing 'wrongful gain to one person or he wrongful loss to another person, is said to do that thing dishonestly.

The fraudulent act need not necessarily be dishonest though it is generally so. The definition of term dishonesty includes wrongful gain or Wrongfull loss actually caused in that sense, fraud is basically that dishonest act which causes wrongfulGain or wrongful loss to parties involved.

As far as bank frauds are concerned the following persons can commit them

- . By the employees of the bank
- . By the employees of the bank in collusion with the outsiders.
- . By outsiders

NOW WE ARE READY TO UNDERSTAND HOW FRAUDS & SCAMS HAVE OVERHELM INDIA

- 1) **The Harshad Mehta Scam:** In 1992, stockbroker Harshad Mehta manipulated the Indian banking system to take advantage of a loophole in the security trading system, resulting in a fraud of around Rs. 4,000 crores. He borrowed money from several banks using fake bank receipts and then invested the money in the stock market, artificially driving up stock prices. The scam came to light when the Reserve Bank of India discovered the fake bank receipts and cracked down on the fraud, resulting in the collapse of several banks and financial institutions.

- 2) **The Satyam Scandal:** In 2009, Satyam Computer Services, a leading Indian IT company, was found to have engaged in accounting fraud and falsification of financial statements to inflate profits and revenue. The scam resulted in a loss of around Rs. 14,000 crores and led to the collapse of the company.

- 3) **The Nirav Modi PNB Fraud:** In 2018, the Punjab National Bank was defrauded of over \$2 billion by diamond merchant Nirav Modi and his associates. The fraud involved the fraudulent issuance of letters of undertaking (LOUs) by PNB employees to companies associated with Nirav Modi, enabling him to obtain credit from overseas banks

Online Banking Fraud: With the increasing use of technology in banking, online banking fraud has become a major concern in India. Fraudsters use various tactics such as phishing attacks, malware, and social engineering to gain access to customers' bank accounts and steal money.

To combat fraud and scams in the banking industry, the RBI has introduced various measures such as the implementation of strict KYC norms, mandatory reporting of fraud incidents, and the creation of specialized departments to investigate financial crimes. Additionally, banks have also invested in advanced security technologies and fraud detection systems to prevent such incidents from occurring.

CAUSES OF FRAUD & SCAMS IN BANKING SECTOR

- 1) **Weak internal controls:** Poor internal controls in banks can make it easier for fraudsters to exploit vulnerabilities and commit fraud. This includes inadequate segregation of duties, insufficient verification procedures, and weak audit trails.
- 2) **Collusion:** Collusion between bank employees and fraudsters is another significant cause of fraud in the banking sector. This can involve bank employees providing confidential information, altering records, or approving fraudulent transactions in exchange for bribes.
- 3) **Lack of training and awareness:** Banks may not have adequate training programs in place to educate employees on fraud detection and prevention techniques. This can make it more difficult for employees to recognize suspicious activity and report it to the appropriate authorities.
- 4) **Rapid expansion of the banking sector:** India's banking sector has experienced rapid growth in recent years, which can lead to a strain on resources and an increase in fraudulent activity. This includes inadequate staffing levels, inadequate IT infrastructure, and a lack of regulatory oversight.
- 5) **Insider trading:** Insider trading involves the use of confidential information by bank employees or other insiders to make a profit or gain an advantage in the stock market. This can involve leaking confidential information to third parties or using it to make personal investments.
- 6) **Cybersecurity risks:** With the increase in digital banking and online transactions, banks face an increasing risk of cyber attacks. Hackers can steal personal information, hijack accounts, and execute fraudulent transactions, leading to significant financial losses.

7) Lack of transparency: Banks that lack transparency in their operations and decision-making processes are more vulnerable to fraud and scams. This includes a lack of disclosure of financial information, hidden fees and charges, and undisclosed conflicts of interest.

8) Non-compliance with regulations: Banks that fail to comply with regulatory requirements are more likely to face legal and financial penalties, as well as reputational damage. This includes failure to report suspicious transactions, lack of due diligence in customer onboarding, and non-adherence to KYC/AML regulations.

9) Poor risk management: Banks that do not have effective risk management strategies in place are more likely to face losses due to fraud and scams. This includes inadequate risk assessment, lack of risk monitoring, and insufficient contingency planning.

10) Social engineering: Social engineering involves the manipulation of individuals to gain access to confidential information or to convince them to carry out fraudulent transactions. This can include phishing scams, vishing scams, and smishing scams.

11) Insider threat: Insider threat involves fraudulent activities carried out by employees of the bank or by individuals with privileged access to the bank's systems and information. This includes embezzlement, data theft, and identity theft.

12) Lack of accountability: Banks that lack accountability in their operations and decision-making processes are more vulnerable to fraud and scams. This includes a lack of oversight by the board of directors, lack of whistleblower protection, and lack of legal enforcement.

WHAT WE LEARN FROM THIS CAUSES

The causes of fraud and scams in the banking sector of India highlight the importance of effective risk management strategies, regulatory compliance, and transparency in operations. Banks need to establish strong internal controls, implement effective risk management strategies, and comply with regulatory requirements to prevent fraud and scams.

It is also important to provide training and awareness programs to educate employees on fraud detection and prevention techniques, and to establish a culture of accountability and transparency within the organization. Banks need to take a holistic approach to risk management, considering both internal and external risks, and implementing appropriate measures to address each type of risk.

Moreover, banks need to adopt robust cybersecurity measures to protect against cyber attacks, which are becoming increasingly common in the digital age. This includes implementing security protocols, educating customers on cybersecurity best practices, and investing in technology that can detect and prevent cyber threats.

In summary, banks in India need to adopt a proactive approach to fraud prevention and risk management, focusing on establishing strong internal controls, compliance with regulations, employee training and awareness, cybersecurity, and a culture of transparency and accountability. By doing so, they can help protect themselves and their customers from the negative impact of fraud and scams in the banking sector.

IMPACT OF FRAUD & SCAMS ON BANKING SECTOR

Fraud and scams have a significant impact on the banking sector of India, both in terms of financial losses and reputational damage. Here are some of the major impacts:

1) Financial Losses: Banks and financial institutions in India have suffered significant financial losses due to fraud and scams. For example, the Nirav Modi PNB fraud case resulted in a loss of over \$2 billion for the bank, and the Satyam scandal caused a loss of around Rs. 14,000 crores.

2) Reputational Damage: Fraud and scams can also damage the reputation of banks and financial institutions, leading to a loss of customer trust and confidence. This can result in a loss of business and revenue, as customers switch to other banks or financial institutions.

3) Regulatory Scrutiny: Fraud and scams can also lead to increased regulatory scrutiny and penalties. The Reserve Bank of India and other regulatory authorities may investigate incidents of fraud and scams and impose fines or other penalties on banks and financial institutions found to be in violation of regulations.

4) Operational Disruption: Fraud and scams can also disrupt the normal operations of banks and financial institutions, leading to delays in services and transactions, as well as increased administrative costs related to investigations and legal proceedings.

5) Impact on the Economy: Fraud and scams can also have a broader impact on the economy of India, as they can undermine investor confidence and discourage foreign investment. This can lead to a slowdown in economic growth and development.

To mitigate these impacts, banks and financial institutions in India need to adopt strong risk management practices, invest in advanced fraud detection technologies, and implement effective measures to prevent and detect fraud and scams. Additionally, regulatory authorities need to impose strict penalties on those found guilty of fraud and scams to deter such activities in the future.

IMPACT OF FRAUD ON CUSTOMERS

The impact of fraud on customers can be significant and long-lasting.

1) Financial losses: One of the most immediate and obvious impacts of fraud on customers is financial losses. When fraudsters gain access to a customer's bank account or credit card, they can use it to make unauthorized purchases, transfer funds, or withdraw money, resulting in financial losses for the customer.

2) Damage to credit scores: Fraudulent activities can also damage a customer's credit score, which can impact their ability to obtain credit in the future. This can be especially harmful for customers who are in the process of applying for loans or credit cards.

3) Time and effort spent on recovery: Customers who have been victims of fraud often spend a significant amount of time and effort trying to recover their losses and restore their credit. This can involve contacting their bank or credit card company, filing disputes, and providing documentation to support their claims.

4) Emotional impact: Fraud can also have an emotional impact on customers, causing feelings of anxiety, stress, and anger. Customers may feel violated or vulnerable, and may lose trust in the banking system.

5) Reputation damage: If a customer's personal information is stolen as part of a fraud scheme, it can damage their reputation and potentially harm their personal and professional relationships.

6) Fear of using services again: After experiencing financial loss and the emotional trauma of being a victim of fraud, customers may feel hesitant to continue using banking services or may choose to switch to a different bank altogether. This fear can be especially pronounced if the customer feels that their bank did not adequately protect them from fraud or respond quickly enough to their concerns.

DETECTION & PREVENTION TECHNIQUE

Detection and prevention techniques refer to the methods and strategies used to identify and stop malicious activities, such as cyber attacks, fraud, and physical security threats. Here are some commonly used detection and prevention techniques:

- A) Firewalls:** A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It can prevent unauthorized access to a network and protect against malware and other threats.
- B) Intrusion Detection Systems (IDS):** An IDS is a software or hardware solution that detects and alerts administrators to unauthorized access or malicious activity on a network or computer system. It can also help to identify and stop attacks before they cause damage.
- C) Access Control:** Access control is the process of regulating who can access a particular resource or system. This can include using passwords, biometric authentication, or other forms of authentication to ensure that only authorized users can access critical resources.
- D) Encryption:** Encryption is the process of encoding data in a way that only authorized users can read it. Encryption can help to prevent unauthorized access to sensitive data, such as passwords, credit card numbers, and other personal information.
- E) Physical Security:** Physical security techniques include measures such as security cameras, access controls, and security guards to protect physical assets, such as buildings, data centers, and other critical infrastructure.
- F) Patching and Updating:** Regularly patching and updating software and systems can help to prevent vulnerabilities and exploits from being used by attackers. This includes updating operating systems, web browsers, and other software on a regular basis.
- G) Education and Training:** Education and training programs can help to raise awareness about security threats and best practices for preventing attacks. This can include training employees on how to identify and report suspicious activity, as well as educating users on how to create strong passwords and avoid phishing scams.
- H) Antivirus Software:** Antivirus software is a program designed to detect and remove malicious software, such as viruses, worms, and Trojan horses. It scans files and other data for known malware signatures and behavior patterns and can quarantine or delete infected files.
- I) Security Information and Event Management (SIEM):** SIEM systems collect and analyze security event data from various sources to identify and respond to security incidents. They can also provide real-time alerts and reports to help security teams investigate and remediate incidents.

J) Network Segmentation: Network segmentation involves dividing a network into smaller subnetworks or segments to reduce the impact of a security breach. By separating critical systems and applications from less critical ones, organizations can limit the scope of an attack and prevent attackers from moving laterally across the network.

K) Penetration Testing: Penetration testing is a simulated attack on a system or network to identify vulnerabilities and weaknesses. It can help organizations to proactively identify and remediate security flaws before they are exploited by attackers.

L) Incident Response Plan: An incident response plan outlines the steps an organization should take in the event of a security incident or breach. It can include procedures for identifying and containing the incident, notifying stakeholders, and conducting a post-incident analysis to prevent future incidents.

M) User Behavior Analytics (UBA): UBA uses machine learning algorithms to analyze user behavior and detect anomalous activity that may indicate a security threat. It can help to identify insider threats, such as employees who are abusing their privileges or attempting to exfiltrate sensitive data.

By implementing a combination of these techniques and regularly reviewing and updating security measures, organizations can better protect themselves against a wide range of security threats.

REGULATORY FRAMEWORK

Regulatory Framework means the Act, Regulations, By-laws, Rules of Professional Conduct and Policies of the Association.

The regulatory framework for the banking sector in India is primarily governed by the Reserve Bank of India (RBI), which is the central bank of the country. The RBI is responsible for regulating and supervising the banking sector, including the prevention of fraud and scams.

Some of the key regulations and guidelines that banks in India need to comply with include:

- 1) Know Your Customer (KYC) norms: KYC norms require banks to verify the identity of their customers and maintain accurate records of their personal and financial information. This helps prevent money laundering, terrorist financing, and other illegal activities.
- 2) Anti-Money Laundering (AML) guidelines: AML guidelines require banks to implement risk-based procedures for detecting and preventing money laundering and terrorist financing activities. This includes establishing internal controls, conducting customer due diligence, and reporting suspicious transactions to the authorities.
- 3) Fraud detection and reporting: Banks are required to establish robust internal controls and monitoring systems to detect and prevent fraud. They are also required to report any suspicious transactions to the relevant authorities, including the Financial Intelligence Unit (FIU).
- 4) Cybersecurity guidelines: The RBI has issued guidelines on information security, electronic banking, and cybersecurity, which banks must follow to protect their customers' personal and financial information from cyber threats.
- 5) Capital adequacy norms: Banks are required to maintain a minimum level of capital adequacy to ensure that they can absorb potential losses and continue to operate in a safe and sound manner.
- 6) Corporate governance guidelines: The RBI has issued guidelines on corporate governance, which require banks to establish a strong internal control system, maintain transparency in their operations, and ensure accountability at all levels of the organization.

These are some of the key regulatory frameworks that banks in India need to comply with to prevent fraud and scams in the banking sector. The RBI periodically reviews and updates these regulations to ensure that they remain relevant and effective in the changing banking landscape.

CASE STUDIES

1) Global Trust Bank Scandal: In 2004, Global Trust Bank (GTB) was involved in a scandal where it was found that the bank's CEO and senior management had colluded with stockbrokers to manipulate the stock market. The scam involved the creation of fictitious accounts, circular trading, and insider trading. The bank was eventually acquired by Oriental Bank of Commerce (OBC) due to its deteriorating financial position.

2) Satyam Computers Scandal: In 2009, Satyam Computers, a leading IT services company, was involved in a scandal where its founder and CEO had inflated the company's financial results by falsifying its accounts and inflating revenue and profits. The scam was uncovered when the CEO confessed to the fraud and resigned. The scandal led to a severe loss of investor confidence in the Indian IT sector and raised questions about the quality of corporate governance practices in Indian companies.

3) Vijay Mallya and Kingfisher Airlines: In 2012, Kingfisher Airlines, owned by businessman Vijay Mallya, began defaulting on loans from several banks, including State Bank of India (SBI). Investigations revealed that the airline had misrepresented its financial position to obtain the loans and had diverted funds for other purposes. Mallya left the country in 2016, and the banks have been trying to recover the loans since then.

4) Bank of Baroda Scam: In 2015, Bank of Baroda was involved in a scam where several employees of the bank allegedly colluded with an external party to transfer \$757 million illegally to Hong Kong. The scam involved the misuse of the SWIFT system to send fraudulent messages to other banks. The scam was uncovered when a whistleblower alerted the authorities, and investigations revealed that the bank had not followed proper procedures for verifying the authenticity of the transactions.

5) Punjab National Bank (PNB) Fraud: In 2018, PNB was involved in a \$1.8 billion fraud, where several employees of the bank colluded with a diamond merchant to issue fraudulent letters of undertaking (LoUs) and foreign letters of credit (FLCs). The scam involved the misuse of the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system to send fraudulent messages to other banks.

The scam was discovered when the diamond merchant failed to repay the loans, and investigations revealed that the bank had not followed proper procedures for issuing LoUs and FLCs.

6) ICICI Bank Scandal: In 2018, ICICI Bank was involved in a scandal where its CEO was accused of nepotism and conflict of interest in lending practices. The CEO had allegedly approved loans to a company owned by her husband's business associate, despite concerns over the creditworthiness of the company. The scandal raised questions about corporate governance practices at the bank and led to an investigation by the regulatory authorities.

7) Yes Bank Scam: In 2020, Yes Bank was involved in a scam where its founder and CEO allegedly colluded with a company to siphon off funds from the bank. The scam involved the misuse of the bank's loans and investments to benefit the CEO and his associates. The scam was discovered when the bank faced a liquidity crisis, and investigations revealed that the CEO had not followed proper procedures for risk management and corporate governance.

These are some examples of fraud and scams in the banking sector in India, and they highlight the importance of effective risk management strategies, regulatory compliance, and transparency in operations to prevent such incidents.

FUTURE OUTLOOK

The future outlook for the banking sector in India with regards to fraud and scams is challenging, but there are also opportunities for growth and improvement. Here are some potential trends and developments to watch out for:

1) Cybersecurity: With the increasing use of technology in banking, cyber threats and online fraud are expected to become more sophisticated and frequent. Banks and financial institutions will need to invest in advanced cybersecurity measures to protect their customers' data and assets from cyber attacks.

2) Regulatory Measures: Regulatory authorities are expected to introduce stricter regulations and penalties to prevent fraud and scams in the banking sector. This could include mandatory reporting of fraud incidents, increased scrutiny of financial transactions, and stricter KYC norms.

3) Fraud Detection Technologies: Banks and financial institutions will need to adopt advanced fraud detection technologies such as artificial intelligence, machine learning, and blockchain to detect and prevent fraud and scams in real-time.

4) Customer Education: Educating customers about the risks of fraud and scams and how to protect themselves will be crucial for preventing such incidents. Banks and financial institutions can provide training and resources to help customers identify and report fraud.

5) Collaboration and Partnerships: Collaboration and partnerships between banks and financial institutions, regulatory authorities, law enforcement agencies, and technology providers will be critical for preventing and detecting fraud and scams in the banking sector.

6) Collaboration with Fintech Companies: Fintech companies are increasingly playing a significant role in the Indian banking sector, and they can offer advanced technological solutions to prevent fraud and scams. Banks and financial institutions can collaborate with fintech companies to leverage their expertise and develop innovative fraud prevention and detection technologies.

7) Focus on Employee Training and Awareness: Fraud and scams can also be prevented by increasing employee awareness and providing regular training on fraud prevention measures. Banks and financial institutions can conduct regular training sessions for employees on how to detect and prevent fraud and scams.

8) Embracing Blockchain Technology: Blockchain technology offers significant potential for preventing fraud and scams in the banking sector. It can create a transparent, decentralized ledger that cannot be altered, making it easier to detect and prevent fraudulent transactions. Banks and financial institutions can leverage blockchain technology to enhance their security and reduce the risks of fraud and scams.

9) Enhancing Customer Verification and Authentication: Customer verification and authentication are essential for preventing fraud and scams. Banks and financial institutions can implement stronger customer verification and authentication measures such as biometrics, two-factor authentication, and digital signatures to ensure that transactions are secure and reliable.

10) Developing Advanced Data Analytics Capabilities: Banks and financial institutions can leverage data analytics to detect and prevent fraud and scams in real-time. By analyzing large volumes of data, banks can identify suspicious patterns and take immediate action to prevent fraudulent activities.

In summary, while the future outlook for the banking sector in India with regards to fraud and scams is challenging, banks and financial institutions can adopt proactive measures to mitigate the risks and enhance their resilience.

These are just a few examples of the potential trends and developments that banks and financial institutions in India can adopt to prevent and detect fraud and scams in the future. By embracing new technologies, collaborating with industry partners, and investing in employee training, banks and financial institutions can enhance their resilience and stay ahead of the ever-evolving threats of fraud and scams.

INTERNATIONAL PERSPECTIVE

An international perspective is an important aspect to consider when studying fraud and scams in the banking sector. Here are some key concepts that can be included under this section:

1) Global impact: This section should highlight the global impact of fraud and scams in the banking sector, including notable cases and their impact on the global financial system. It should also explore the differences in the prevalence and types of fraud in different regions.

2) Regulatory differences: This section should explore the regulatory differences between different countries in the banking sector, including the strengths and weaknesses of regulatory frameworks in different regions. It should also discuss how international standards, such as those set by the Basel Committee on Banking Supervision, impact regulatory frameworks in different countries.

3) International cooperation: This section should discuss the efforts being made at an international level to combat fraud and scams in the banking sector. This can include the role of international organizations such as the Financial Action Task Force (FATF), Interpol, and the World Bank in setting global standards and facilitating cross-border cooperation.

4) Cross-border fraud: This section should explore the challenges of preventing and detecting cross-border fraud and scams in the banking sector. This can include issues related to jurisdiction, information sharing, and cooperation between law enforcement agencies in different countries.

5) Best practices: This section should highlight best practices from around the world for preventing and detecting fraud and scams in the banking sector. This can include the adoption of technology and innovative risk management practices. It should also discuss the potential benefits of sharing best practices across borders and between different regions.

WHAT IS CONTRIBUTING TO RISE IN FRAUD

Fraud tends to be committed primarily due to the presence of three major factors: financial pressure, opportunity, and rationalization. While these factors are present in a growing economy, they can get exacerbated during an economic downturn, when margins are tight and profitability is a challenge. This has been clearly brought out in our survey results, where respondents have attributed the increase in fraud to the lack of oversight by line managers or senior management on deviations from existing process/controls; business pressure to meet targets; and collusion between employees and external parties.

The results indicate that **lack of training, overburdened staff, competition, and low compliance level**, the degree to which procedures and prudential practises framed by the Reserve Bank of India to prevent frauds are followed are the primary reasons for bank frauds. More factors are....

Increasing digitization: As banking services become more digitized, fraudsters are finding new ways to exploit vulnerabilities in digital systems to execute fraudulent activities.

Lack of awareness: Many customers and employees may not be aware of the various types of bank fraud and the measures they can take to protect themselves from fraudsters.

Weak internal controls: Banks may have weak internal controls or oversight, which can make it easier for employees or agents to engage in fraudulent activities.

Poor cybersecurity: Banks may have poor cybersecurity measures in place, such as weak passwords or outdated software, which can make it easier for cybercriminals to gain access to sensitive information.

Organized crime: Organized criminal networks may engage in bank fraud as a means to generate illicit profits, using sophisticated techniques and networks to execute large-scale fraud schemes.

It is important for banks and other financial institutions to implement robust fraud prevention measures, including training employees and customers, implementing strong cybersecurity measures, and conducting regular risk assessments to identify vulnerabilities and mitigate potential risks.

ANALYSIS

As per the RBI, bank frauds can be classified into three broad categories: deposit related frauds, advances related frauds and services related frauds.

Deposit related frauds, which used to be significant in terms of numbers but not in size, have come down significantly in recent years, owing to a new system of payment, and introduction of cheque truncation system (CTS) by commercial banks, use of electronic transfer of fund, etc.

Advances related fraud continue to be a major challenge in terms of amount involved (nearly 67 percent of total amount involved in frauds over last 4 years), posing a direct threat to the financial stability of banks. With ever-increasing use of technology in the banking system, cyber frauds have proliferated and are becoming even more sophisticated in terms of use of novel methods. Also, documentary credit (letter of credit) related frauds have surfaced causing a grave concern due to their implications on trade and related activities.

The data reveals that more than 95 percent of number of fraud cases and amount involved in fraud comes from commercial banks. Among the commercial banks, public sector banks account for just about 18 percent of total number of fraud cases, whereas in terms of the amount involved, the proportion goes as high as 83 percent. This is in stark contrast with private sector banks, with around 55 percent of number of fraud cases, but just about 13 percent of the total amount involved in such cases (Figure 1). The PSBs are more vulnerable in case of big- ticket advance related frauds (1 crore or above) in terms of both number of fraud cases reported and total amount involved (Figure 2).

The correlation between rising level of NPAs of public sector banks and frauds probably indicates lack of requisite standards of corporate governance leading to more instances of high value bank loan default and possible collusion between corporate entities and high Rank bank officials.

Figure 1: Group wise summary of bank fraud cases

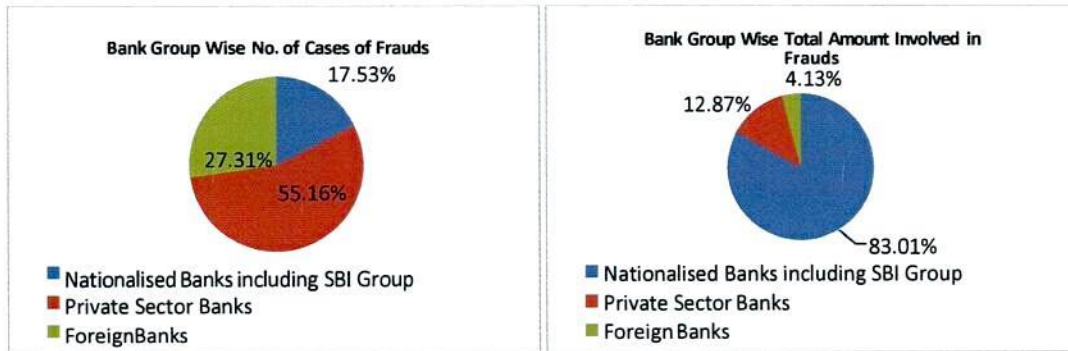


Figure 2: Group wise summary of advance related fraud cases



According to findings of Deloitte (2015), number and sophistication of frauds in banking sector have increased over the last two years. Around 93 percent of respondents suggested an increase in fraud incidents and more than half said that they had witnessed it in their own organizations. Retail banking was identified as the major contributor to fraud incidents, with many respondents saying that they had experienced close to 50 fraudulent incidents in the last 24 months and had lost, on an average of Rupees ten lakhs per fraud.

The risks undertaken by banks are still a cause of worry although it has moderated a bit. This is indicated by the bank stability indicator. Similarly, banks were worried by poor asset quality. Further, the ratio of stressed assets has increased significantly in the last few years.

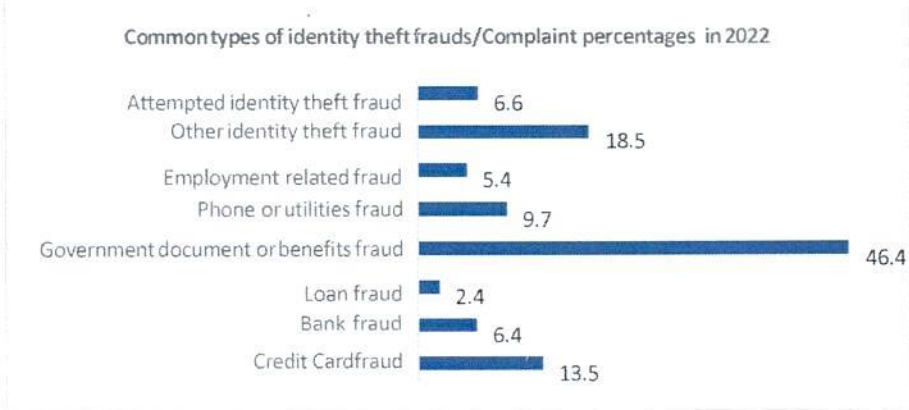
As far as credit risk is concerned, 16 out of 60 banks (26.5 percent market share) were not able to cover their expected losses from their current framework.

RBI states that NPAs from retail banking are just 2 percent, whereas NPAs from corporate banking are 36 percent. Given the size of transactions in corporate banking, it is important that banks implement a robust monitoring mechanism post sanction and disbursement of facilities, and be vigilant to early signs of stress in the borrower accounts.

India has witnessed a massive surge in cybercrime incidents in the last ten years.

As per the government's cyber security arm, computer emergency response team-India (CERT-In), 62,189 cyber security incidents were reported in just the first five months of 2021-22.

Figure 4: Identity Theft Fraud



Interview Based Finding

A semi-structured interview was conducted by the authors with various officials of the banking industry and investigating agencies. Detailed projects can be made available on request. Thus, from the study, the authors were able to come up with the following insights and key findings:-

1. **Fraud detection procedure in public sector banks:** The authors analyzed the process of fraud detection and reporting in a public sector bank and who are the various players involved in this process. Following is a step by step illustration of the same (Figure 5).
 - a) First, a fraud is internally reported to senior management of a bank. These may include chief general managers, executive directors, chairman and managing director. They may also be reported to vigilance department of the bank.
 - b) If reported to the vigilance department of the bank, it investigates the fraud and then reports it to both senior management as well as the central vigilance commission (CVC) to whom they are required to report monthly.
 - c) Although CVC can report fraud directly to investigating agencies like CBI, usually final decision to either report fraud to an external agency or to deal with it internally is made by senior management of the bank. Depending upon size of bank, amount of money involved in fraudulent activity and number of the third involved, senior management may choose to deal with the fraud internally or file an FIR and report it to either local police or CBI.
 - d) A committee of the RBI also independently monitors fraudulent behaviour in banks and reports its observations on quarterly basis to central board of the RBI. The board may then report the matter to either central vigilance commission or ministry of finance (MoF).
 - e) Auditors, during the course of their audit, may come across instances where transactions in accounts or documents point to possibility of fraudulent transactions in accounts. In such a situation, auditor may immediately bring it to the notice of top management and if necessary to audit committee of board for further action appropriate action.

- f) Employees can also report fraudulent activity in an account, along with the reasons in support of their views, to the appropriately constituted authority (Table 1), under the whistle blower policy of the bank, who may institute a scrutiny through the fraud monitoring group (FMG). The FMG may 'hear' the concerned employee in order to obtain necessary clarifications. Protection should be available to such employees under the whistle blower policy of the bank so that fear of victimization does not act as a discouragement.

Flow Chart depicting procedures post Fraud Detection and Reporting in PSBs



Current Structure for filing Police/CBI complaints

Category of Bank	Amount Involved in the Fraud	Agency to whom complaint should be lodged	Other Information
Private Sector/ Foreign Banks	Rs.1 lakh and above	State police	
	Rs.10000 and above if committed by staff	State police	
	Rs.1 crore and above	Serious fraud investigation office (Ministry of Corporate Affairs)	In addition to state police
Public Sector Banks	Below Rs. 3 crore	State police	
	Rs.3 crore and above and up to Rs.25 crore	CBI	Anti-corruption branch of CBI (where staff involvement is prima facie evident) Economic offences wing of CBI (where staff involvement is prima facie notevident)
	More than Rs.25 crore	CBI	Banking Security and Fraud Cell (BSFC) of CBI (irrespective of the involvement of a public servant)

Source: Reserve Bank of India.

- 4) **Reason for higher advance related frauds in public sector banks and rising NPAs:** Higher advance related frauds of above Rs. one crore loans (87 percent of total amount involved in loan worth Rs. one crore or above in value) (Figure 2) in public sector banks as compared to private sector banks (11 percent of total amount involved) could be due to the proportion of the loan advanced by both PSBs (~ 70 percent) and private sector banks (~ 30 percent) especially in large and long gestation projects like infrastructure, power or mining sectors. Also, the higher number of fraud cases reported by PSBs (65 percent of total) as compared to PVBs (19 percent of total) may be attributed to stringent oversight of CVC in PSBs. It may also be due to a possible underreporting/evergreening of loans on the part of the PVBs, evidenced by RBI's measures to curb such practices in recent times.

The reason for large NPA's of PSBs could be attributed to greater amount of lending/exposure to mining, infrastructure and power sector projects, whose performance and associated cash flows closely follow the economic cycle of boom and recession. Also, in India, post - 2008 global crisis, a number of governance and other external issues such as policy paralysis, inordinate delay on account of stringent environmental laws/regulation, Supreme Court decision on coal mines as well as weak demand crippled these sectors and resulted into weaker cash flows. These developments severely affected the ability of such firms to service their loans leading to higher NPAs.

- 5) **Third party agencies involved:** Big loan advance frauds are not so easy to commit and it often results because bank officials collude with borrowers and sometimes even with officials of third parties such as advocates or chartered accountants (CAs). In such cases, the third parties such as the CAs or the advocates often get away as it is nearly impossible for the banks to prove criminal intent on the part of such persons due to various reasons such as lack of clear understanding of legal matters to bankers, and lack of expertise and legal advice on this subject, and unwillingness to reveal some sensitive data to courts/ public domain. Also, self-regulatory bodies of advocates, auditors or accountants like bar council and the institute of chartered accountants of India do not generally bar their errant members.

Auditors Can Be

A) **Bank auditors** – There are two main types of auditors that work for a bank to look into financial statements of its borrowers. They work in different capacities in terms of their scope and knowledge. They can be held responsible for any misreporting under common legal framework due to faith placed on them by banks.

The two Main types of auditors are:

i. **Statutory auditor** – These look into financial statements of all borrowers that borrow from a bank. These are external auditors.

ii. **Concurrent auditor** – These help supplement the functioning of bank in terms of internal checks and check on financial statements of its borrowers. These maybe external/internal auditors

B) **Statutory auditors of the borrower** – These auditors work for the borrower firm and help in reporting their financial statements.

C) **Special auditors** – These auditors work on a case by case basis independently and are not associated with any firm or bank. They help provide an external view on statements reported by the borrower to the bank.

- 6) **Poor appraisal system and monitoring mechanism in PSBs:** The initial project appraisal process in PSBs is as good as that of PVBs. But monitoring post sanction of loan is weaker in PSBs compared to the PVBs on account of diverse loan portfolio, lack of expertise and modern technological resources, and lack of manpower and motivated employees, who are not appropriately incentivized to detect early frauds or prevent them.
- 7) **Corporate governance and other HR issues:** The root cause of weak corporate governance at highest level is directly linked to the very process of appointment of highest level of officials and poor compensation structure of highest level functionaries. Also, there is a serious issue in terms of pay structure in higher rank of PSBs, which is markedly lower than their counterparts in PVBs. The only good factor in PSBs is prestige of a post that a person holds.

The inability to hire competent professionals and expertise from market (lateral hiring) due to existing recruitment policy, flight of officials to greener pastures and private or foreign banks, poor compensation structure, unionization challenges as well as lack of adequate training in contemporary fraud prevention techniques are key HR issues, which indirectly contribute to bank frauds.

If the case is finally taken up in the court of law, a public prosecutor represents the bank. The public prosecutor is usually overburdened with pending cases. Additionally, from the bank's perspective, having already lost substantial amount in fraud, they allocate limited budget for prosecutions, making it easier for the guilty to escape.

8) **Bank employees:** Incentive structure for employees needs a re-evaluation and gives too much importance to short term targets. This incentivizes the employees to give preference to short term targets only and not exercise proper due diligence. Hence, they take more risk than is usually the norm or resort to unethical means. There have been instances of frauds involving collusion of staff with third party agents like auditors to indulge in fraudulent activities on customers. Detection of such frauds takes a long time, and is only discovered when there are customer complaints of fraudulent cases. The customers who are victim of fraudulent activities by the bank, due to identity theft etc., could have avoided so, by following appropriate preventive measures and customer awareness guidelines. Political reasons may also be responsible for indulgence in loans proceed which has substantial risk of being defaulted or defrauded, especially when a red flag is raised on the loan. As legal opinion is not the strength of a banker, advocate's directions in that matter assume importance.

Frauds also result from lack of awareness of staff towards appropriate procedures in place and red flags they should be aware of. Technology related frauds are primarily due to non-adherence to standard procedures and systems in place, by the employees. Even when any employee detects some fraudulent activities in existence involving people in power, whistle blower protection policy does not guarantee adequate safety.

PSBs in India had prepared a five point action plan to make them more competitive, which included suggestions like introduction of performance management systems and incentives in banks. Smaller banks should focus on the areas of their strength (to optimize capital utilization) among other reform plans.

9) **Borrowers and clients of banks:** Frauds may also arise solely from the borrower's side. Companies have been found to take part in 'high sea sales' with investment from Indian banks but the funds are either routed for other purpose or are not repaid after the sale has been made and instead, routed to other channels, resulting in a NPA. Such breach of contract is another instance of fraud since the funds are not utilized for the purpose they were initially set out and based on the project evaluated by the banker.

10) **Legal aspects of frauds and role of investigative agencies:** Investigating and supervisory bodies like central vigilance commission (CVC) or central bureau of investigation (CBI) are already overburdened with many pending investigations and have limited resources at their disposal.

The biggest hurdle in pursuing fraudsters is proving criminal intent on their part in the court of law. Most of the bank frauds are detected very late and by that time, fraudsters get enough time to wipe out trails and it becomes very difficult to establish criminal intent due to loss of relevant documents and non-availability of witnesses.

Also, while pursuing fraudsters, banks and investigation agencies face many operational issues. Bankers are not experts in legal paperwork, and formal complaints against fraudsters drafted by them often lack incisiveness. Also, in absence of a dedicated department handling fraud matters, investigating officers (CBI/police) have to deal with multiple departments and people within the bank, which often results into poor coordination and delay in investigation.

This results in very low conviction rate for fraudsters (less than 1 percent of total cases). Even after conviction in fraud cases, there is no legal recourse to recover the amount lost in the bank frauds and the country's legal system is perceived to be very soft on defaulters. Also, lack of strong whistle-blower protection law inhibits early detection in case of involvement of internal Employees.

11) **Judicial system:** The long and elaborate judicial process is another major deterrent towards timely redressal of fraud cases. The delay in judiciary to prosecute those guilty of fraudulent practices, could lead to dilution of evidence as well as significant cost building on part of the victim bank.

Also, wilful default is still not considered as a criminal offence in India. Fraudsters, both big and small, take undue advantage of these means of evasion and commit maligned activities without risk of conviction.

12) **Technological and coordination perspective:** RBI has an elaborate set of early warning signals (EWS) for banks to curtail frauds. However as of now, there are inadequate tools and technologies in place to detect early warning signals and red flags pertaining to different frauds. The authors' interaction with a former chairman of a big public sector bank shockingly revealed that there is only one provider of vigilance and monitoring software for banks and price discovery is poor. Even the biggest of public sector banks cannot afford to buy that software. Also, lack of coordination among different banks on fraud related information sharing is another major roadblock.

LESSON TO BE LEARNED FROM SCAM

(ESPECIALLY FROM HARSHAD MEHTA SCAM)

Large-scale financial scams have occurred even in the most modern banking system. International experience shows that, in most of these cases, there has been lack of adequate supervision by the regulatory authorities and collusion between the bank employees and the perpetrators of fraud. The financial scam, which surfaced in India in April 1992, has been investigated and these investigations have brought to light the underlying economic factors and inadequacies in the system, which were exploited by the scamsters. All dark clouds have a silver lining. A scam of this dimension does contain many lessons for the future. The lessons could be drawn from the experience for evolving suitable remedies at the Government level, Regulator level and Institutional level. The developments since 1992 indicate that right action was not taken based on the lessons available from the experience in a number of areas. The fact that a number of scams arising out of the same set of causes did take place since 1992 - Hawala Scam, MS Shoes scam, CRB Capital Scam and scams in the Cooperative banks in Gujarat and Andhra - showed that the remedial measures were either not taken or they were inadequate.

ADEQUACY OF PRESENT LAW

Fraud is not defined anywhere in the IPC sections. It is defined in Indian Contract Act Sec.17

Fraud means and includes any of the following acts committed by a party to a contract, or with his connivance, or by His Agent, with intent to deceive another party there to or his agent, or to induce him to enter into the contract:

The suggestion, as to 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

Why fraud has not been dealt with in Indian Penal Code sections is not clearly understood probably the existence of sections dealing with Cheating (Secs. 415 to 420), Concealment (Secs. 421 to 424), Forgery (Secs. 463 to 477A), Counterfeiting (Secs. 489A to 489E), Misappropriation (Secs. 403, 404) and Breach of Trust (Secs. 405 to 409) must have been thought to be adequately covering the frauds.

But there is a need to differentiate between the fraud under civil law and a criminal fraud. A fraud in the civil sense means:

“the successful practice of deception or artifice with the intention of cheating or injuring another, Ordinarily fraud involves willful misrepresentation, the deliberate concealment of a material fact for the purpose of inducing another person to do or to refrain from doing something to his detriment, or the failure to disclose a material fact. Thus a person may be fraudulently misled into giving up a claim to property, waiving legal rights or entering into a disadvantageous contract”

The same sense is meant as per the Indian Contract Act also. But the element of crime such as Cheating, Concealment, Forgery, Counterfeiting, Misappropriation and Breach of Trust, etc. is not present in that definition. It is imperative in the present day world circumstances that fraud be defined as comprehensively as it is needed for the day.

In the meanwhile, the present law has the following sections to deal with frauds

Cheating

IPC Sec. 415 Definition of cheating

IPC Sec. 416 Definition of cheating by personation

IPC Sec. 417 Punishment for cheating — One year imprisonment or with fine or with both

IPC Sec. 419 Punishment for cheating by personation — Imprisonment for three years or with fine or with both

IPC Sec. 420 Cheating and dishonestly inducing delivery of property — punishment —imprisonment for seven years and with fine

IPC Sec. 421 Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors — Punishment- Imprisonment for two years or with fine or with both

IPC Sec. 422 Dishonestly or fraudulently preventing debt being available for creditors
Punishment — Imprisonment for two years, or with fine , or with both

IPC Sec.423 Dishonest or fraudulently preventing debt being available for creditors

IPC Sec. 424 Dishonest or fraudulent removal or concealment of property — Punishment — Imprisonment for two years or with fine or with fine or with both

Forgery

IPC Sec. 463 Definition of Forgery

IPC Sec. 464 Making a false document

IPC Sec. 465 Punishment for Forgery — Imprisonment for two years or with fine or with both

IPC Sec. 466 Forgery of valuable security, will, etc. — Punishment — Imprisonment for seven years and shall also be liable to fine

IPC Sec. 467 Forgery of valuable security, will, etc. — Punishment — Imprisonment for seven years and shall also be liable to fine

IPC Sec. 468 Forgery for purpose of cheating — Punishment — Imprisonment for seven years and shall also be liable to fine

IPC Sec. 469 Forgery for purpose of harming reputation – punishment
Imprisonment for three years and shall also be liable to fine

IPC Sec. 470 Definition of Forged document

IPC Sec. 471 Using as genuine a forged document

Counterfeiting

IPC Sec. 472 Making or possessing counterfeit seal, etc., with intent
to commit forgery, punishable under section 467

IPC Sec. 473 Making or possessing counterfeit seal, etc., with intent
to commit forgery, punishable otherwise — Punishment~
Imprisonment for seven years and shall also be liable to fine

IPC Sec. 474 Having possession of document described in section 466 or 467
knowing it to be forged and intending to use it as genuine —
Punishment — Imprisonment for seven years and shall also be liable
For fine

IPC Sec. 475 Counterfeiting device or mark used for authenticating
documents described in section 467, or possessing
counterfeit marked material — Punishment – Imprisonment: for seven
for seven years and shall also be liable to fine

IPC Sec. 476 Counterfeiting device or mark used for authenticating documents other
than those described in section 467, or possessing counterfeit marked
or possessing counterfeit marked material – Punishment —
Imprisonment for seven years and also to fine

IPC Sec. 477	Fraudulent cancellation, destruction, etc., of will, authority to adopt or valuable security — Punishment — Imprisonment for seven years and shall also be liable to fine
IPC Sec. 477A	Falsification of accounts — Imprisonment for seven years, or with fine, or with both
IPC Sec. 489A	Counterfeiting currency-notes or bank notes - Punishment — Imprisonment: for ten years and shall also be liable to fine
IPC Sec. 489B	Using as genuine, forged or counterfeit currency-notes or bank notes ~ Punishment — Imprisonment for ten years and shall also be liable to fine
IPC Sec. 489C	Possession of forged or counterfeit currency notes or bank-notes — Punishment — Imprisonment for seven years, or with fine, or with both
IPC Sec. 489D	Making or possessing instruments or materials for forging or counterfeiting currency notes or bank-notes — Punishment ~ Imprisonment for ten years and shall also be liable to fine
IPC Sec. 489E	Making or using documents resembling currency-notes or bank-notes — Punishment — fine

Misappropriation

- IPC Sec. 403 Dishonest misappropriation of Property — Punishment —
Imprisonment for two years, or with fine, or with both
- IPC Sec. 404 Dishonest misappropriation of property possessed by
deceased person at the time of his death — Punishment
~Imprisonment for seven years

Breach of Trust

- IPC Sec. 405 Definition of Criminal breach of trust
- IPC Sec. 406 Punishment for criminal breach of trust — Imprisonment
for three years, or with fine, or with both
- IPC Sec. 407 Criminal breach of trust of carrier, etc. — Punishment —
Imprisonment for seven years, and also shall also be liable to fine
- IPC Sec. 408 Criminal breach of trust by clerk or servant —
Punishment — Imprisonment for seven years and shall to fine
- IPC Sec. 409 Criminal breach of trust by public servant, or by banker,
merchant or agent — Punishment — Imprisonment for
ten years, and shall also be liable to fine

Robbery and Dacoity

IPC Sec. 390	Definition of Robbery
IPC Sec. 391	Definition of Dacoity
IPC Sec. 392	Punishment for Robbery — R.I. for 10 to 14 years and fine
IPC Sec. 393	Punishment for Attempt to commit Robbery ~7 years plus fine
IPC Sec.394	Punishment for voluntarily causing hurt in committing Robbery — Imprisonment for Life or R.I. for 10 years plus fine
IPC Sec. 395	Punishment for Dacoity — Imprisonment for Life or R.I. for 10 years plus fine
IPC Sec. 396	Punishment for Dacoity with Murder — Imprisonment for Life or R.I. for 10 years plus fine
IPC Sec. 397	Punishment for Dacoity with attempt to cause death or grievous hurt — Imprisonment for 7 years

Criminal Conspiracy

- IPC Sec.120A Definition of criminal conspiracy
- IPC Sec.120B Punishment of criminal conspiracy - Imprisonment
For 2 years or more

The Criminal Procedure Code, 1973

- Cr.P.C. Sec.292 Evidence of the officers of the Mint
- Cr.P.C. Sec.293 Reports of certain government scientific experts like
Chemical Examiner or Assistant Chemical Examiner of
the Government, Director of the Finger Print Bureau,
Director of the Central Forensic Science Laboratory, etc.

The Indian Evidence Act, 1872

- IEA Sec.32 Statement by person who is dead or cannot be found
- IEA Sec.45 Opinion of experts like experts in foreign law, science or
art or handwriting or fingerprints, etc.
- IEA Sec.46 Facts bearing upon opinions of experts
- IEA Sec.51 Grounds of opinion when relevant
- IEA Sec.57 Facts of which court must take judicial notice
- IEA Sec.58 Facts admitted need not be proved
- IEA Sec.60 Oral evidence must be direct
- IEA Sec. 73 Comparison of signature, writing or seal
- IEA Sec. 159 Refreshing memory

The Indian Contract Act, 1872

ICA Sec. 17 Definition of Fraud

ICA Sec. 72 When delivery of money is made by a mistake or under coercion

The Reserve Bank of India Act, 1934

RBIA Sec. 13 Restriction on issue of demand bills a notes

The objective of the Paper Currency Act to prevent banks and private persons from infringing on the government monopoly of issuing of the paper currency in India

The Negotiable Instruments Act, 1881

NIA Sec. 45A Holders right to duplicate of lost bill

NIA Sec. 58 Instrument by unlawful means or for unlawful consideration

NIA Sec. 85 Cheque payable to order

NIA Sec. 87 Effect of material alteration

NIA Sec. 138 Dishonour of cheque

NIA Sec. 139 Presumption in favour of holder

NIA Sec.140 Unacceptable defence

NIA Sec. 141 Offences by companies

NIA Sec. 142 Cognizance of offence

LESSON TO BE LEARNED FROM SCAM AT GOVERNMENT LEVEL

The scam surfaced at a time when the government was contemplating a series of economic reforms relating to capital markets, banking sector, insurance, telecom, power and transport. It is to be noted that the peak period of the financial scam - April 1991 to May 1992 - coincided with the period of introduction of deregulation measures in the financial sector.

It is not advocated that the then existing "Over regulated and under-governed" financial system should have been allowed to continue as such. However, such a system was responsible to a considerable extent for the origin of the irregularities in the transactions of securities by circumventing and violating the rules. There was a need to change such a system. Where things went wrong was in the way in which the financial sector reforms were ushered in and handled ineptly.

The results of investigations clearly indicated that government should take remedial action in five major areas. They are

- A) Regulation of Markets through reform measures
- B) Ensuring adequate legal framework to deal effectively with the offenders,
- C) policy decision relating to financial sector
- D) coordination and interface among the different agencies and
- E) introducing transparency and accountability in financial transactions.

DOES THIS DATA MAKE ANY MEANING

Like for instance in the Harshad Mehta Scam, the CBI recorded a number of cases which were actually sequential in nature. Meaning thereby that all the offences, which were recorded as separate cases, could have been bundled together to be a single case. Since the CBI found that a single case would be neither easy for investigation nor for coherently charge sheeting them in court, has found out the most convenient way of splitting the transactions and recording them as separate cases.

Given the unpredictability of the time-lagged effect on involvement in fraud and on the filtering of the cases through the policing and prosecution process, it would be hard to build up an econometric model of the relationships between fraud and the volume and/or profitability of business. The problems of reporting behaviour and of policing resources and attitudes would bedevil the validity of any such model. However, the extent of frauds money-wise have increased more than five times from 2015 to 2020 which is both alarming and serious in nature.

The scale of losses or injuries does not determine how we will react to any given type of conduct. If we did, we would pay more attention to road traffic accidents and less to dacoity and intentional murder.

All sorts of things affect the way we view and react to social harms. Apart from the physical and financial impact some factors such as the perceived intent of the person who is seen as causing the harm is also important. Statistics are often deployed a form of propaganda.

Being the harshad mehta scam of stock manipulation it affected market in this way



WAYS OF DEFRAUDING

There are many ways of defrauding in which the following are the major ones.

Forged Signatures: Forgery of signatures is the most important fraud. Nearly seventy percent of the cheque frauds are forgery of signatures. Bankers come across signatures in a number of situations.

Signatures of customer/fagent on cheques

Specimen signatures of the account holders

Signatures of bankers on drafts or on bankers cheques

Signature of bankers on mail transfer orders

Signatures on collection bills, discounted bills, etc.

Signatures on miscellaneous documents like deposit receipts,

Vault register, receipts, charge reports, etc.

Endorsements of holders of instruments

Signatures on travelers cheques

Signatures on credit cards

Signatures on hypothecation documents

Signatures on loan agreements

All signatures are highly personal and individualistic. They are a person's graphic identity. Forged signatures are written to usurp the personality of the victim or one's own personality. Forgery involves a clear-cut criminal intent and has been defined in Indian law in sections 463 and 464 IPC.

Genuine signatures of a person on a document are the symbol of the authority one confers on that document. They give sanctity to the contents of that document. The banker generally comes across genuine signatures only. But he has to be doubly sure about the signatures.

Normal characteristics in brief

The speed and abandon with which signatures are made by a person. It is indicated by flying start and finish. Graduated pressure, which varies with the movement of the pen and the line strokes, which are free of defects.

Rhythm which flows of his pen is automatically characterized by unhindered flow of the writing, usual emphasis on certain letters or parts of the stroke, direction of writing line, letter proportions, executing loops, curves, etc.

In genuine signatures there are natural variations and there is certainly no attempt to hide them or to correct them. The variations are within a well defined range.

There is a personal subconscious emphasis on certain letters, strokes and construction. This appears in enlarged sizes or ornamentation.

There are highly individualistic directional movements of the pen to form letters, combination of letters or connectives.

Spacing is also highly individualistic.

Size of the letters, words or their abbreviations are highly characteristic. Placements of dots, full stops, dashes, etc. though inconspicuous are very individualistic.

Forging of signatures has acquired the status of an art and science.

Forgery of signatures is committed in a number of ways. Bank Frauds in India

① **Simulated signatures:** This is the most common method of forgery by carefully copying a model signature of a victim, which can be variously called as copy forgery, imitation forgery, free hand forgery or simulated forgery.

② **Traced signatures:** Being a replica of a model they are easily mistaken for the genuine signatures. The following techniques are used:

③ **Indented tracing:** the model signature is being placed over the document being forged and a pencil or pen or any other instrument is moved along the line of the signature with adequate pressure to cause an indentation. In another method tracing paper is placed over the model signature. The traced signature is transferred to the actual document in the indented outline obtain is inked.

④ **Simulated signatures:** This is the most common method of forgery by carefully copying a model signature of a victim, which can be variously called as copy forgery, imitation forgery, free hand forgery or simulated forgery.

⑤ **Traced signatures:** Being a replica of a model they are easily mistaken for the genuine signatures. The following techniques are used:

A) **Indented tracing:** the model signature is being placed over the document being forged and a pencil or pen or any other instrument is moved along the line of the signature with adequate pressure to cause an indentation. In another method tracing paper is placed over the model signature. The traced signature is transferred to the actual document in the indented outline obtain is linked.

B) **Carbon tracing:** a carbon paper is placed between the model signature and the document being forged. The pen or pencil or stylus is moved along a line of model signature with adequate pressure. Carbon line obtained on the document is inked.

C) **Transmitted light tracing:** A glass piece is illuminated from underneath by an electric lamp. The model signature to be copied is placed on the glass piece and the document being forged is placed over the model signature. The position of the document is adjusted in such a way that a model signature appears at the desired site. The optical outline is linked.

D) **Projection tracing:** Projection equipment is used to obtain a real image of the model signature on a screen. The document being forged is placed on the screen. The projected image outline appearing on the document is linked.

E) **Pantograph tracing:** A pantograph is a device used for duplicating a graphic design. This can be used to duplicate signatures.

⑥ **Signatures by trickery:** In forgery by trickery the signatures of victim are genuine. They are obtained by trickery and false representation.

Such signatures are generally obtained in the following situations:

Signatures obtained on blank papers, cheques, etc by false representation

Signatures obtained on unimportant documents leaving large spaces between the text and signature to trim the text later on and utilize the signatures by forgery

⑦ **Signatures by Scanning:** This is the most modern way of copying the signatures with the use of computers. The document containing the signature is scanned using a Scanner and the required signature is transferred to any document unto which the signature is supposed to be affixed, The signature thus obtained may be traced up to make it appear genuine.

MAJOR LESSONS

Based on the experience of the Scam of 1992, one can draw three major lessons for regulating the markets. The first one is, before introducing deregulation; the government should ensure that checks and balances are built in the system. Deregulation does not mean no regulation. Unnecessary curbs in the market should have been removed and an orderly trading to protect the interests of the public should have been introduced by a system of efficient re-regulation.

It is rather unfortunate that this was not followed while attempting the reforms in the Insurance sector, Telecom sector and Power sector. Insurance Regulatory Authority was created without statutory powers and the legislation for the same took quite some time. In the case of TRAI it was set up, dissolved and re-introduced in a different form thereby causing considerable delay in implementing reforms. Similar was the story with respect to regulatory authorities in power sector, which is yet to take off in the Centre and the States. It is strange that the government has accepted the necessity for regulatory reforms but the implementation is quite tardy. The second lesson is that the regulatory set up should not have gaps. The lack of proper regulatory authorities for UTI, NBFCs and NHB was the main reason for irregular transactions in these institutions. Here again, action to rectify was haphazard, slow and ineffective. SEBI did not have control over all the operations of UTI. The overseas corporate bodies (OCBs) did not come under the purview of either SEBI or RBI. A number of NBFCs exploited these grey areas. For proper governance in the financial sector, the government should ensure that there is no area in the system, which is not governed by any statutory regulations. The third lesson is to develop a monitoring and warning system in the Ministry of Finance, to keep a close watch on the development of the markets, analyze the signals professionally and advice the government in time. Nobody can question the need for it. But this is yet to materialize.

LEGAL LEARNINGS

The biggest handicap in handling the scam was the absence of a legal system through which the scamsters could be dealt with expeditiously. When the scam surfaced in April 1992, the Government had no other way than to issue an ordinance, since the existing law did not have a definition for offences relating to securities. It is to be noted that even with the Special Court ordinance, it took nearly 7 years to get the first conviction (which went in appeal to Supreme Court). This situation has to be compared with that of Singapore where the accused in the Baring Bank case was apprehended, prosecuted and convicted within a period of one year. Government did realize the need to have a comprehensive legislation for dealing with economic offences and initiated steps. However, very little progress has been made and it is reported that the proposed legislation "is being processed in consultation with all concerned". The fact remains that till date we do not have an adequate legal frame work in place.

Transparency and Accountability

In the banks and financial institutions the transactions in securities were handled by a small group of officials in the treasury department and even the chief executive and the Board of Directors were not aware of the system and procedure followed. All the senior managers while giving evidence before the IPC admitted that these transactions lacked transparency. When even those who were holding top managerial positions did not know the operations, the quantum of irregularities naturally increases in volume. This situation got worse in the absence of accountability and the size of the scam transactions further increased. It appears government followed the culture of non-accountability without openly declaring it as a policy. It is to be noted that the ethos of non-accountability had got into the financial system so strongly that it continued even after the exposure of the scam. Even though assurances were given in the Parliament to deal with those found guilty, the recommendations and indictments of the JPC were handled in a way, which clearly showed that the Government was not very keen on taking action against those who were indicted. The Action Taken Report (ATR) tabled by the Government was quite evasive and in effect did not accept the concept of accountability at higher levels. Government was reluctant to proceed against the top management of RBI, the Ministries and the Ministers even though the JPC report clearly indicted them. It is because of this reason that the ATR failed to convince anyone and lacked credibility.

The pertinent point to note is that the Government could see the basic issue of the culture of non-accountability in varying degrees in the handling of all these scams. It is this culture that led to several public interest litigations and the subsequent interference by the Judiciary giving directions to the executives as also monitoring compliance.

The basic reason for this "Judicial Activism" is the callousness shown by the executive wing by adopting the policy of non-transparency and non-accountability. The accounting system, the balance sheet, the system of provisioning for non-performing assets, selection of broker and investment policy is to be evolved based on the concept of transparency. Transparency in the system and transactions will lead to questions and the demand for scrutiny of operations.

If such scams are to be avoided in future, the one and only way is to ensure that the concept of transparency and accountability are followed in the letter and spirit. The developments after the scam indicate that even though the emerging lessons from the scam and the recommendations of the JPC are accepted, in actual practice the concept of accountability does not appear to be followed and action taken in a convincing way. The occurrence of scams at regular intervals proves the point. One can only hope that the public opinion will prevail and things will improve in the future.

Financial Institutions Findings

The financial intermediaries which played a key role in the scam of April 1992 were scheduled commercial banks in the public and private sector, foreign banks, cooperative banks, Bombay Stock Exchange and non-banking financial companies, such as Fair Growth Financial Services Ltd, CANFINA, ABFSL and SBI Caps. The most important lesson that emerges for the financial intermediaries based on the experience of the scam is that of ensuring an effective system for internal monitoring control and vigilance.

The irregularities could continue for nearly seven years undetected, because the internal control system and monitoring were either absent or did not function. The management did not exercise any control and handled the inspection reports in a casual and callous manner. In State Bank of India the Deputy Managing Director in charge of treasury was made to continue in the same post beyond three years against the normal guidelines regarding rotation in senior posts for the simple reason that he played a key role in getting good profits from the transactions in Government securities.

The top management never bothered to inspect the department or question the procedure followed or verify whether the transactions were in accordance with the rules and guidelines. After the scam surfaced it came out that the Chairman and the Board of Directors were not even aware of what was actually happening. No senior official who appeared before the Joint Parliamentary Committee ever admitted to knowing what was happening.

ROLE OF A BANKER IN PERPETRATION OF FRAUDS

Any banker's mind is prioritized consciously or subconsciously in the following manner;

- A) Getting very good deposits
- B) Meeting his targets
- C) Earning good profits
- D) Outshine his competitors

Getting good deposits for the bank is the basic aim of all bankers. This is set as a benchmark for good performance and is fed into the basic psyche of every banker. In most cases, the colour of money that a banker is after does not matter for him. He considers a person who has deposited large amounts in his bank to be a good customer. He does not even blink his eyelid once to pry on his good customer's sources of money. It can be black money, illegal money, and any kind of money for that matter. He even grants unnecessary and indiscriminate loans to such kind of people by mentioning them as his good customers in the credit worthiness reports in their loan assessment forms.

All this is done just because he wants to boost his deposit figures. This attitude of bankers trying to pass off large amount depositors as good customers has been encouraging fraud, This tendency also encourages people to acquire money by any means.

Meeting targets is the next important priority on the mind of a banker. He is so very claustrophobic over this thought that nothing matters much to him as he goes along to 'somehow' meet those targets. Year-ending window dressing of balance sheets is a very common phenomenon in almost every bank. Bankers go to any lengths to attain their targets. This encourages corruption and fraud. Loans are given without proper verification while rules and procedures are just a mangled mess.

The third objective of earning good profits puts a banker on the same plane of thinking of that of a conventional small time businessman. He just wants to earn more, come rough weather or rains.

Basically, banking is a business proposition. A banker has to earn profits for his survival. But paradoxically, the nationalization of public sector banks had put him in a Catch 22 situation. He has to meet the social obligation of developing the society on the one hand, and yet earn his bread and butter. To ean better he takes higher risks and runs into bad times more often. This is when frauds take place.

FRAUD PRONE AREAS

It is a fact that all the connected people to frauds,. (a) banker (b) fraudster and (c) the regulatory body, know which areas are prone to frauds. The areas are so elaborately publicized that sometimes it is felt that it is so much necessary to do so.

Even in the name of education! In this age of publicity overkill and training, all and sundry come to know about the fraud prone departments in banks and the modus operandi of frauds to the last detail. It only takes one to pick up a classic case and just replay the whole act afresh in a virgin and unexplored place and situation. And lo and behold, there is a fresh fraud on hand.

Umpteen number of fraud cases are just repetitions of what had already occurred before, Does that mean one should not publicize the cases of fraud? The answer to this is both Yes and No.

It is yes because if the concerned people do not know how frauds take place, how would they avoid/prevent/tackle them in future. Certainly, fraud prone areas must be known to all concerned as also the modus operandi being used in committing frauds to enable them cope with very effectively.

CONCLUSION

The performance of public sector banks (PSBs) in India over the past few years has been mixed, with some banks reporting losses while others reported profits. However, the overall trend has been one of increasing losses, mainly due to higher provisioning for non-performing assets (NPAs), which has been a persistent problem for the banking sector in India.

The COVID-19 pandemic has further exacerbated the situation, leading to an increase in loan defaults and a slowdown in economic activity. It is clear that PSBs in India need to address the issues of NPAs and improve their risk management practices in order to improve their financial health and contribute to the growth of the economy.

The government has taken several steps in this direction, such as the recapitalization of PSBs and the introduction of various reforms, but more needs to be done to ensure the long-term sustainability of the banking sector in India.

Credit related frauds have the maximum impact in all the banking frauds in India because of the high amount involved and the cumbersome process of fraud detection followed by CVC.

RECOMMENDATIONS

The frauds may be primarily due to lack of adequate supervision of top management, faulty incentive mechanism in place for employees; collusion between the staff, corporate borrowers and third party agencies; weak regulatory system; lack of appropriate tools and technologies in place to detect early warning signals of a fraud; lack of awareness of bank employees and customers; and lack of coordination among different banks across India and abroad.

The delays in legal procedures for reporting, and various loopholes in system have been considered some of the major reasons of frauds and NPAs.

Despite efforts, banks have not been very successful in conviction of individuals responsible for financial crimes. One of the root causes of this problem is identified as lack of specialized financial sleuths with knowledge of nuances of forensic accounting as well as a good legal understanding of frauds

Therefore, following recommendations are suggested for an early detection of fraud

A) Independent specialized Group: The government could consider an independent specialized cadre of officers on the lines of all India services, who are equipped with the best financial and legal know-how to detect financial frauds and are capable of carrying out an effective and time bound investigation of such scams. In short term, the government can consider forming this cadre with a pool of commercial bankers, RBI and CBI officials through lateral recruitment.

B) Know your markets: In addition to know your vendor and know your customer, the banks should also focus on know your markets. There should be a dedicated cell within each bank to assess the company/firm to which they are lending and the macro-economic environment of the concerned industry or market where products are marketed. This recommendation even seems relevant in the context of the recent crash of the Chinese market. Several Indian manufacturing companies, which were dependent on import of machinery from China, could not start their projects and generate cash flows, and this in turn affected the banks from which loans were raised.

C) Internal rating agency: Banks should have a strong internal rating agency, which evaluates big ticket projects before sanctioning loan. The rating agency should strictly evaluate the project on the basis of business model/plan of project without being influenced by brand name or credit worthiness of the parent company, considering current macro-economic situation and exposure of the sector to the global economy. In case ratings of internal and external agencies are not similar then an investigation must be conducted to establish the causes for such differences. Also, bank should seek services of at least 2-3 independent auditors in evaluation of such projects so as to prevent chances of any possible collusion.

D) Use of latest technology: The data collection mechanism in banks is very archaic and needs a revision. The banks should employ the best available IT systems and data analytics in order to ensure effective implementation of the redflagged account (RFA) and early warning signals (EWS) framework suggested by the RBI, which would help in a better profiling of customers by analysing patterns of their transactions and rendering a near real time monitoring possible for banks. Also, we recommend that the Institute for Development and Research in Banking Technology (IDRBT) could consider incentivising development of relevant software for commercial banks at affordable costs. This is vital to enhance their monitoring of suspicious and fraudulent transactions within the branches of their banks.

E) Monitoring outlier movement at regional level: The RBI could consider extending its monitoring ambit and scope, and should monitor the outlier movements of transactions at regional level on the lines of SEBI's circuitbreaker, which might be effective in tracking the earliest possible signs of financial frauds.

F) Strong punitive measures for third parties: The government should consider examining the role of third parties such as chartered accountants, advocates, auditors, and rating agencies that figure in accounts related to bank frauds, and put in place strict punitive measures for future deterrence. There is also a case to be made to question the certification/credentials of third parties like auditors to decide their competence in evaluating accounts containing potentially fraudulent entries.

G) Strong laws to prevent fraudulent financial reporting: There are many areas where the current laws can be made stronger to improve accountability of auditors toward their jobs.

- i. One of them could be strengthening KYC norms: A benchmark in this case can be guidelines issued by OECD to regulate trust and corporate service providers (TCSPs) that helped extend liability of fraudulent malpractices in these institutions to lawyers and auditors as well. In India, NBFCs are required to act similarly by reporting about suspicious transactional activities but this is not done effectively as these laws are very weak in their current form.
- ii. Another law that can be strengthened is that of wilful default which should be made a criminal offence. It is currently a civil offence under Indian law, whereas it is a criminal offence in other countries.

H) Ground intelligence assets: Banks should be equipped with some intelligence gathering agency, which might be deployed to track activities of borrowers and is able to help the bank in ensuring real time compliance and early detection of fraud. A special fraud monitoring agency should be setup in banks with highly skilled/trained officials. A specialized investigating agency is also needed with expertise from agencies such as CBI, RBI, SEBI and commercial banks.

I) Dedicated department for handling fraud cases: There should be a dedicated department equipped with legal assistance in every corporate branch of a PSB, which serves as a single point of contact with investigating agencies and facilitates easy access to relevant documents.

J) Financial literacy: Many a times, staff does not know the exact definition of fraud and thus needs to be educated regarding this aspect. Therefore, learning sessions for employees and the best practices across the world in areas of early fraud detection and prevention should be imparted to staff on regular basis. There can be regular e-modules with e-certifications and updates made available.

K) Transparent hiring and adequate compensation: Banks have to ensure corporate governance at the highest levels. Top management needs to set guidelines and policies for ethical practices and standard procedures to be followed throughout and set an example on zero tolerance to negligence and fraudulent activities. Considering the roles and responsibilities of top management, emphasis should be given on appropriate hiring procedure at top management level, with appropriate preference for minimum service of at least 3 years, with accountability clause. Also, changes need to be incorporated on incentive mechanisms to have a balance between short term and long term targets.

In I would like to say that is crucial to focus on strengthening risk management practices, improving the quality of loan assets, embracing digital technology, encouraging innovation and entrepreneurship, strengthening governance and accountability, and collaborating with other stakeholders.

By adopting these measures, they can improve their operational efficiency, enhance customer experience, reduce costs, and contribute to the growth of the economy. The government has taken several steps in this direction, but more needs to be done to ensure the long-term sustainability of the banking sector in India.

SPECIAL COURTS FOR FINANCIAL & BANK FRAUDS

These courts should be in the pattern of Special Courts (Trial of Offences relating to Transactions in Securities) Act 1992. There will be a Special Court of this nature in each State. It will consist of a sitting Judge of the High Court nominated by the Chief Justice of the High Court within the local limits of whose jurisdiction the Special Court is situated, with the concurrence of Chief Justice of India.

This Special Court shall take cognizance of or try such cases as are instituted before it or transferred to it which are connected with financial or banking frauds. The Special Court will have jurisdiction to try cases which fall under the head of Financial and Banking Frauds as presently covered by IPC, PC Act 1988, Indian Evidence Act 1872, Indian Contract

Act, Reserve Bank of India Act 1944, Negotiable Instruments Act 1881, etc.

THIS IS HIGHLY RECOMMENDED

BIBLIOGRAPHY

Here is a list of sources that I have used to write my project on the topic of Bank fraud in India:

Reserve Bank of India Annual Report:

<https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?year=2021>

Economic Times:

<https://economictimes.indiatimes.com/industry/banking/finance/banking/bank-fraud/articleshow/74182577.cms>

Business Today: <https://www.businesstoday.in/current/economy-politics/bank-fraud-cases-in-india-jump-28-per-cent-in-fy21-rbi/story/440303.html>

Cyber Crime Investigation Cell (CCIC):

<https://www.cybercrimeinvestigationcell.com/>

Indian Banks' Association: <https://www.iba.org.in/>

National Crime Records Bureau: <https://ncrb.gov.in/>

Ministry of Home Affairs: <https://www.mha.gov.in/>

PwC India Report on Economic Crimes:

<https://www.pwc.in/assets/pdfs/publications/2020/pwc-economic-crimes-survey-2020.pdf>

Deloitte India Report on Financial Crimes:

<https://www2.deloitte.com/in/en/pages/financial-services/articles/india-financial-crime-report.html>

KPMG India Report on Cybercrime:

<https://home.kpmg/in/en/home/insights/2020/12/cybercrime-survey-2020.html>

These sources provide valuable insights into the current state of bank fraud in India, the trends, the impact, and measures being taken to prevent and combat it.

OpenAI. (2021). ChatGPT [Computer software]. GitHub.

<https://github.com/openai/gpt-3>

Obviously all the sites were not used in project but I have mentioned some sites where one can get the Info