GOVERNMENT DEGREE COLLEGE, HAYATHNAGAR

DEPARTMENT OF COMMERCE

JIGNASA STUDENT STUDY PROJECT

TOPIC :DIGITAL BANKING FRAUDS –A CASE STUDY IN TELANGANA

STUDENTS

1	ASRA FARHEEN	B.COM II YR
2	B.MAHESHWARI	B.COM II YR
3	T.VENKATESH	B.COM II YR
4	B.MALLIKA	B.COM II YR
5	K.TEJASRI	B.COM II YR

SUPERVISOR :DR GUNDETI SUNITHA

PRINCIPAL :DR K JYOTSNA PRABHA

1.1 **INTRODUCTION:**

Research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically. In it we study the various steps that are generally adopted by a researcher in studying his research problem along with the logic behind them.

Research is a very general term for an activity that involves finding out, in a more or less systematic way, things you did not know. A more academic interpretation is that research involves finding out about things that no-one else knew either. It is about advancing the frontiers of knowledge. Research is an academic activity and as such the term should be used in a technical sense. According to Clifford Woody research comprises defining and redefining problems, formulating hypothesis or suggested solutions; collecting, organising and evaluating data; making deductions and reaching conclusions; and at last carefully testing the conclusions to determine whether they fit the formulating hypothesis.

1.2 REVIEW OF LITERATURE:

Banking system in the modern times have become the backbone of any economy and the need for quality banking with robust risk management has been the concern of not just economists but also the legislators. One of the biggest problems in recent times has been that of Banking Frauds, both internal and external, and many Laws and Regulations have been enacted. Fraud' has been broadly defined in various Laws to include deliberate acts to cause either unlawful gain to oneself or unlawful loss to another, however, Banking Fraud has not been specifically defined, resulting in difficulties at the enforcement level, due to the multitude of activities that may be encompassed within its ambit Research in the area of Banking has been more focused on the aspects of the development of Banking Systems and Laws and Banking Frauds find a brief mention. The Researcher referred to various Books, Research Papers, Journal Articles, Newspaper Reports, Surveys published by Scholars from myriad fields like Economics, Management, Sociology, Psychology and Law. Some of the relevant literature reviewed has been discussed below.

One of the earliest works on the issue of Bank Fraud, that was reviewed, was A Treatise on Saving Banks...' (1860) by **Arthur Scratchley**[1] in which the author enumerated numerous instances of Bank Fraud that were reported in United Kingdom during the mid-

1800s. The author emphasized that frauds originated due to lack of an appropriate audit and review system of the banking practices and negligence of the Trustees and Mangers of the banks. His work shows that frauds in the Banking Sector are not new and have rather been in existence since the beginning of the Banking Business.

In India**, V. R. Solanker's** [2]Book Banking Frauds in India', highlighted cases of frauds in the Banking Sector after establishment of RBI under the Reserve Bank of India Act, 1934. In this Book, Solanker elucidated the vulnerabilities in the banking operations and practices which provided opportunities of frauds like fake drawers of hundis, discounting of bills of exchange, embezzlement etc. Solanker's work in this area is noteworthy as the frauds and vulnerabilities of banks underlined in his Book were in the backdrop of the set of RBI with the objectives of providing financial stability, regulating the financial structure and operating the credit system in India.

B R Sharma[3], in the first edition of his Book Bank Fraud: Prevention & Detection,' published in 1984, covered the subject of Bank Fraud prevalent in India and the third edition published in 2009 has updated the same to cover the modern-day Banking Frauds involving E-Banking frauds. The Book discusses the legislative and administrative measures that were introduced in response to the growing cases of E-Banking Frauds. Dr Sharma presents apractical guide which compiles the nature, modus operandi of Banking Frauds and the measures available to combat and mitigate the losses caused by these.

R.P. Nainta[4], in his Book, dealt with the diverse aspects of the banking system in India, the role of RBI and legislations in controlling Bank Fraud. He has discussed the security aspects in E-Banking and the measures that have been taken to address the vulnerabilities posed due to ever evolving technology. According to him, a sound banking system should have a fraud free culture, a best practice code and an effective in-house grievance redressal system, which he finds are either missing or weak within the Indian Banking System.

Sharma and Brahma[5] focused their Research on the responsibility of a banker in Bank Fraud and were of the view that, a dishonest banker can play havoc with the bank's money.' They argued that the bank, thus, has to be the watchdog to safeguard its' customers and itself against dishonest employees. According to them, Bank Fraud may be attributed to operational negligence, lax managerial controls, excessive discretionary

powers in advancing credit facilities to valued customers and insider-outsider alliances, wherein bank employees facilitate the perpetuation of fraud by either active concealment of material facts, forgery or leaking sensitive information. They concluded that insiders significantly contribute to Bank Fraud and constant vigilance by banks is the way towards reducing the incidences of Bank Fraud.

Federal Deposit Insurance Corporation (FDIC)[6] in its DSC Risk Management Manual of Examination Policies'31, in its section on Bank Fraud and Insider Abuse, points out that of all the cases of frauds and embezzlement in the Banking Sector in US, closed by the Federal Bureau of Investigation (FBI), insider fraud attributed to more than half of them. The Manual enumerates some of the ways by which insiders or employees abuse the trust for their own gains like related party dealings, diversion of banks resources for personal use, misuse of their position, acceptance of graft for providing services which may have been declined or any dubious transactions related to their position in the organization. The Manual further opines that though detection of all frauds, involving insider abuse, is not possible, probable issues can be ascertained if examiners are alert towards certain warning signs.

Dr. K C Chakrabarty[7], in his Paper, Fraud in the Banking Sector – Causes, Concerns and Cures, concludes that frauds have a greater impact on banking institutions, as they are primary operations necessarily require channelization of funds between depositors and/or investors and borrowers. He further pointed out that Bank Fraud have the potential of resulting in huge economic costs as these can lead to disruptions in the financial markets and payment systems. Moreover, according to him Bank Fraud can weaken the trust of people in the banking system and may sometimes be detrimental to noy only the integrity but also the stability of the economy of any Country. He opined that frauds, can collapse banks, weaken the supervisory role of the banks' regulator, cause unrest and discontent amongst people besides causing political cataclysms. Dr. Chakrabarty was of the view that the recent technological innovations, in the banking services, have further heightened the vulnerabilities of banks to fraud attacks.

Kundu and Rao[8],in their study on reasons behind Bank Fraud, concluded that the occurrence of Bank Fraud could be attributed to untrained employees, lax supervisory/managerial control and situational pressures. The study further found that

frauds are not only difficult to detect while they are ongoing, but their prosecution is also trickier due to complicated legal and judicial procedures. To make matters worse, frauds are often not reported by banks for fear of reputational losses. The delays in reporting and prosecuting of frauds further encourages more people to commit them. The study suggested that for there to be a robust banking system, banks must ensure internal controls that provide for an environment that not only discourages fraud but provides for strict measures against those who perpetuate it and greater use of forensic data analytics to monitor and detect possible fraud risks.

In 2015, **ASSOCHAM and PWC India's**[9] Paper, on Fraud Trends in the Financial Sector, examined the regulatory perspectives, resources and tools for fighting frauds that were being used by financial institutions and found that the changing technology being employed for financial transactions have increased the prospects and motivations to commit frauds that use the technology to their advantage. Frauds like Embezzlement, Identity Theft, Money Laundering to name a few were being perpetuated using complex methodologies. According to their Paper, economic frauds accounted for approximately 20 billion US Dollars in losses and affected foreign investment flows in India. The paper suggested that financial institutions and regulators needed to strengthen their fraud risk management strategies with greater transparency at all levels within the organization.

Bhasin[10] conducted a questionnaire-based Survey of 345 bank employees in the year 2012-13 to ascertain their assessment of frauds in the Banking Sector and the reasons that impacted their levels of compliance and pointed out that with the growth of the banking industry and operations, complex and inventive frauds and fraudulent schemes have also seen a sharp rise. The Survey highlighted that whilst attaining a fraud free banking ecosystem may not be feasible, banks must take the initiative measures to guard themselves against fraud risks by continuous risk assessments of all activities across all banking processes. The Survey found that the most common reasons for non-compliance were ineffective training programs for employees, poor internal controls, lack of administrative oversight and suggested that banks must employ modern technologies like data mining and data forensic tools to combat the emerging complex fraud techniques.

RBI Chair Professor

Charan Singh et al[11], in their Research Paper , 'Frauds in the Indian Banking Industry' concluded that, the main reasons for the growth of frauds in banks could be attributed to inadequate management oversight over operations, skewed incentive procedures for staff, ineffective regulatory controls, absence of proper tools and technologies
for detecting red flags in case of probable frauds, lack of training and education regarding safe banking practices of both employees and customers, employees colluding with corporate customers and third parties to defraud the bank and poor exchange of information amongst banks. The paper further found that besides the above mentioned reasons, delays in detecting, reporting, investigation and the ensuing legal procedures, coupled with the inherent ambiguities in the system have also contributed to the growth of frauds. Lack of specialized investigators, who are trained in financial forensics and legal procedures as well as low conviction rates vis-à-vis financial crimes was identified by the Paper as one of the root causes of increasing frauds in the Indian Banking Industry.
In their third Survey on Banking Frauds,

Deloitte[12] stated that over a period of six years from 2012-2018, Bank Fraud steadily increased in both, number of frauds reported and the cost of losses sustained. The Survey found that the main contributors towards this increasing trend of frauds were, a lack of sufficient usage of forensic analytics for identifying possible red flags among various banking processes, inadequate supervision by managers and top management on employee deviations from set policies and responsibilities and emergence of new technologies and e-platforms making detection of frauds more complex and difficult. The Survey concluded that some degree of risks is integral to the banking business, but banking and financial institutions need to have effective control mechanisms to counter the rising incidents of frauds. Further, internal controls need to be constantly upgraded as they weaken over time owing to advances in the technology, human intercession like supervisory overrides or complicity, or advent of newer fraud stratagems. This Survey suggested that banks should focus on investing more in latest technology for creating better accountability and recognition of preventive measures vis-a vis frauds, carryout comprehensive assessments of their fraud risks and implement robust policies to mitigate them and finally the ecosystem within which these operate must be such that works towards fraud prevention.

1.3 RESEARCH PROBLEM

Digital India is future of the country towards present generation moving rapidly. The technology plays crucial knowledge for driving digital India in different sectors. The proper usage of the digital economy is very inevitable from safety and transparency point of view. The loop holes in technology and poor knowledge of public giving scope to some hackers and fraudulent people to cheat the public and earn money in illegal way. These frauds are growing very fast along with the growth in digital banking. The regulatory bodies of various sectors giving instructions and caution the public against these types of frauds. However, still these frauds are not come up to the control. This issue is addressed in the present study.

1.4 SIGNIFICANCE OF THE STUDY

The digital frauds rate is highly significant in banking sector which causes the loss of money by the public and hamper the public confidence on the digital banking and entire banking sector. However, still banking sector failed in recovery of money and detecting and preventing the accounts of frauds. There is inadequate research studies focused on the types of frauds exposed by the public, pushing factors towards becoming of victims of the banking frauds, examining the impact of banking online frauds on the victims economic status and reactivation rate of digital banking after experience of frauds.

1.5 OBJECTIVES OF THE STUDY

- To study nature and types of digital banking frauds exposed by the public
- To examine impact of digital banking frauds on the economic status of victims in Telangana
- To find out the reactivation rate of digital banking by the victims in Telangana.
- To measure the satisfaction level of victims on response by the banks against complaints
- To elicit the suggestions from the victims for reducing the frauds in digital banking.

1.6 RESEARCH METHOLOGY

Present study is based on both primary and secondary data. The primary data is collected from the targeted victims of digital banking frauds through snow ball sampling technique. Snow ball sampling method is a technique used to identify of the sapling population with help of one and another. This is a non-probability technique and named as chain-referral sampling technique. The data is collected in the month of Novembers 2022 from the targeted victims in Telangana . In the process of data collection I sent questionnaire in Google format to 150 members. Out of 150, I received complete responses from 144 members, but inadequate from two members and four not completely responded. Thus, present study sample size is 144.

1.7RESEARCH INSTRUMENTS/STATISTICAL TOOLS:

- Well Structured Questionnaire
- Percentages

1.8 LIMITATIONS OF THE PRESENT STUDY:

- Present study is confined only to 144 victims in Telangana only.
- The study is focused only on digital frauds in banking sector and ignored other sectors.
- The limited time is one of the constraints.

1.9DATA ANALYSIS AND INTERPRETATION

1.9.1 DEMOGRAPHICA STATUS OF THE RESPONDENTS

Table 01: DEMOGRAPHIC STATUS OF THE RESPONDENTS

Gender of the Respondents		Education of the Respondents		Region of Respondents	
Male	120 (83.3)	Post Graduation	24 (16.7)	Rural	42 (29.16)

Female	24 (16.7)	Graduation	60 (41.7)	Urban	72 (50)
		Intermediate	48 (33.3)	Metropolitan	30 (20.84)
		Others	12 (8.3)		
Total	**144** **(100)**	**Total**	**144** **(100)**	**Total**	**144** **(100)**
Source: Field study					

In the present study demographic status of the respondents is presented in the above table. In the study male participant's rate is 83.3 percent which is significantly higher to female participants 16.7 percent. In the respondents 41.7 percent pursued graduation while 33.3 percent pursued intermediate, 16.7 percent pursued post graduation and only 8.3 percent pursued other educational qualification such as 10^{th}, ITI etc. In the regional wise participation 50 percent of respondents are urban residents, 29.16 percent is rural residents and 20.84 percent participated from metropolitan background. In the study majority of respondents are male, education is above graduation and urban and metropolitan city.

1.9.2 ONLINE BANKING AND MOBILE BANKING USAGE PERIOD OF THE VICTIMS.

Table 02: Online banking and mobile banking usage period of the Victims

Years	Online Banking	Mobile Banking

Less than one year	18 (29.2)	6 (4.2)
1-2 years	42 (23.6)	47 (32.6)
2-3 years	34 (8.3)	12 (8.3)
3-4 years	12 (12.5)	43 (29.9)
Above 4 years	38 (26.4)	36 (25)
Total	144 (100)	144 (100)
Source: Field Study		

In the present study, 29.2 percent of respondents using online banking since less than one year, where 26.4 percent using above since last four years. Similarly, 23.6 percent of respondents using online banking between 1-2 years, 12.5 percent since 3-4 years and 8.3 percent since 2-3 years. On the other hand, another mode of digital banking is mobile banking services, in the total respondents 32.6 percent of respondents using between 1-2 years, 25 percent using since four years, 29.9 percent usage period is between 3-4 years and 8.3 percent using period is between 2-3 years finally 4.2 percent is usage period is below one year. In overall, around 70 percent of respondent's usage period of online banking is above one year where as 95 percent of respondents usage rate of mobile banking is above one years. This indicates that, mobile banking is relatively most convenient mode of customers in Telangana.

1.9.3 Monthly Digital Banking Transactions Size and total loss amount

of the victims

Table No 03: Monthly Digital Banking Transactions Size and total loss amount of the Victims

Sl. no	Size of transaction	Responds	Loss size
1	Above Rs 500000	7 (4.9)	6 (4.2)
2	Rs 100001 -Rs 500000	16 (11.1)	0 (0)
3	Rs 10001-Rs 100000	55 (38.2)	44 (30.6)
4	Less than Rs 10000	66 (45.8)	94 (65.3)
	Total	144 (100)	144 (100)
Source: Field Study Note: value in brackets indicates percentage			

In the present study majority of the respondents i.e. 45.8 percent is monthly digital transactions size is below Rs 10000 followed by 38.2 percent Rs 10001 to Rs 100000, 11.1 percent between Rs 100001-Rs 500000 and lowest is 4.9 percent above Rs 5 Lakhs. This indicates that majority of respondents preferring digital banking for lower amount. On the other hand, the public loss amount in digital banking frauds, around two third is below Rs 10000 due to day transfer limits and low balance in the account. where 30.6 percent loss is in the range of Rs 10001 to Rs 100000 and finally 4.2 percent in the range of above Rs 5 Lakhs. This indicates that majority of victims amount is less than Rs 10000.

1.9.4 VICTIMS REACTIONS AFTER FRAUD DETECTED

Table no: 4 Victims Reactions after fraud detected

	Reaction nature	Yes	Percentage
1	Blocking card/online banking/mobile banking services, changing passwords	132	91.6
2	Complaint to the nearest bank branch	102	70.83
3	Complaint to the cyber crime	63	43.75
4	Simply changing pass words, without complaint	32	22.22
	Total		228.4
Source: Field study			

The study found that 91.6 percent of victims blocking their debit/credit card, online banking and mobile banking after fraud detected, 70.83 percent of respondents are giving complaint near bank branch, 43.75 percent is gave complaint to cyber crime and only 22.22 percent is not giving complaint and simple changing passwords. Majority of the victims are immediately stopping their cards and online/mobile banking services which is best strategy to prevent further loss of money. However, the still few victims are still hesitate to give complaint to branches not very low victims are giving complaint to cyber crimes. Government and banks should encourage the victims to file complaint in near branch and cyber crimes.

1.9.5 NATURE OF DIGITAL BANKING FRAUDS EXPOSED BY VICTIMS

Table no 5: NATURE OF DIGITAL BANKING FRAUDS EXPOSED BY VICTIMs

	Form of fraud	Multiple Responses	Percentage
1	ATM card skimming	42	29.17
2	QR code scan	52	36.11
3	Fake advertisement for loans	62	43.06
4	Asking OTP/CVV	96	66.67
5	Loans with forged documents	23	15.97
6	KYC update calls	103	71.53
7	Account blocked messages	121	84.03
8	SMS/E-mail	73	50.69
9	Others (Please specify	32	22.22
	Total		419.44

In the present study 84.3 percent of victims exposed to account blocked message, 71.53 percent exposed to KYC update calls frauds, 66.67 percent exposed to asking of OTP/CVV, 50.69 percent is getting SMS/E-mail frauds, 43.06 percent getting fake advertisements, 36.11 percent facing QR code scan, 29.17 percent exposed to ATM card skimming and 15.97 percent exposed to loans with forged documents and 22.22 percent exposed to other problems.

1.9.6 COMPENSATION OF VICTIM'S LOSS BY THE CONCERNED BANKS IN TELANGANA

	Particulars	Responses	Percentage
1	Fully compensated	21	14.6
2	Not at all compensated	25	17.4
3	Partially compensated	12	8.3
4	Not Responded	86	59.7
	Total	144	100
Source: Field study			

The survey witnessed that, only 14.6 percent of the victims is compensated their full amount followed by 8.3 percent partially compensated and 17.4 percent is not at all compensated. The major reason for not compensation by the banks is attributable sharing of credentials (OTP and CVV etc) by the victims to strangers. The full compensation was received only the case where bank accounts are hiked without interference of the customers.

1.9.7 VICTIM'S SATISFACTION ON ACTIONS TAKEN BY BANKS AND CYBER CRIMES

	Particulars	Responses	Percentage
1	Highly Satisfied	42	29.2
2	Moderately satisfied	36	25
3	Highly dissatisfied	6	4.2

4	Dissatisfied	24	16.7
5	Not Responded	36	25
	Total	144	100
Source: Field study			

The study measured satisfaction of the victims regarding the banks and cyber crime actions to their complaints the study found that 29.2 percent of the employees only expressed high satisfaction whereas 25 percent expressed moderate satisfaction. In contrast, 16.7 percent expressed dissatisfaction and 4.2 percent expressed highly dissatisfaction. This indicates that, more than half of the victims and those given complaints expressed satisfaction towards banks actions and explanation to their digital banking issues.

1.9.8 IMPACT OF DIGITAL BANKING FRAUDS ON THE FINANCIAL STATUS OF THE VICTIMS

	Particulars	Responses	Percentage
1	Highly significant	18	12.5
2	Significant	48	33.3
3	Moderate	24	16.7
4	Negligible	24	16.7
	Not responded	30	20.8
	Total	144	100
Source: Field study			

The survey examined the impact of bank's frauds on the financial status of the victims. The study revealed that, digital banking frauds have shown significant impact on the financial status of the 33.3 percent of victims, high significant on 12.5 percent, 16.67 percent moderate impact. Another 16.7 percent of victims expressed negligible impact. This reveals that, digital banking showing significant impact on the financial status of the majority of the victims.

1.9.9 VICTIM'S RATING ON THE DIGITAL BANKING USAGE

	Particulars	Responses	Percentage
1	Excellent	24	16.7
2	Good	48	33.3
3	Poor	24	16.7
4	Dangerous	18	12.5
	Not Responded	30	20.8
Total		144	100
Source: Field study			

Finally the study asked the victims of the digital banking victims to rate the digital banking services. The study found that 33.33 percent of the victims expressed "Good" Rating whereas 16.7 percent rated "Excellent". In contrast, 16.50 percent gave "Poor" rating and 12.5 percent gave "Dangerous" Rating.

1.9.10 REACTIVATION OF DIGITAL BANKING SERVICES OF VICTIMS AFTER FRAUDS

		Responses	Percentage
1	Yes	78	54.2
2	No	42	29.20
3	Not Responded	24	16.7
	Total	144	100
Source: Field study			

It is observed that, in total victims 54.2 percent is reactivated digital banking after frauds which indicate that still majority of the respondents are expressing confidence towards digital banking. This response is got majority from victims with lower amount of loss (less than Rs 10000). However, victims of huge losses are not reactivated their digital banking services due to afraid of repeat frauds. This indicates loss confidence on digital banking.

1.10 FINDINGS OF THE STUDY:

- In the present study, male participant's rate is 83.3 percent and female participant's rate is 16.7 percent. The educational back ground of the study revealed that, 41.7 percent of victims pursued graduation, 16.7 percent pursued post graduation and 33.3 percent completed intermediate and 8.3 percent pursued other educational qualification such as vocational. The regional wise participants revealed that, 50 percent of victims are residing in urban areas, 29.16 percent is residing in rural areas and 20.84 percent is living in metropolitan areas.
- The study found that, majority of victims i.e. 53 percent usage period of online banking is less than two years. In contrast, this even uses of mobile banking more than four years are exposed to digital banking frauds due to technological changes in usage and poor awareness on frauds.
- The study found that, majority of the victims of the digital frauds transaction size and loss size is less than Rs 10000 and followed by Rs 100000.

- The study found that, more than 90 percent of victims immediately block their cards after frauds detect while only 22.23 percent is confined only to password changes, 70 percent had given complaint to the nearest branch and 43.75 is giving complaint to cyber crime. This indicates that cards block and approaching near banks are strategies using by the victims.
- The study found account blocked message, KYC calls update and asking OTO and CVV are top three methods of digital frauds exposed by the majority of the victims.
- The study found that, regarding the compensation point of view more than half of the victims did not respond to the question due to their unwillingness. However, 17.4 percent of victims expressed no compensation, 8.3 percent is partially not compensated and 14.6 percent is fully compensated.
- The study investigated that more than half of the victims of the study expressed satisfaction on digital banking services in Telangana.
- The study observed that, around 45 percent of the victims expressed significant impact digital frauds on their economic status and caused short term troubles in life.
- The study found that, even after experience of digital banking frauds more than 40 percent of victims expressed positive opinions on digital banking due to reason that digital banking is good method when properly used with good knowledge.
- It is observed that, in total victims 54.2 percent is reactivated digital banking after frauds which indicate that still majority of the respondents are expressing confidence towards digital banking. This response is got majority from victims with lower amount of loss (less than Rs 10000).

1.11 SUGGESTONS OF THE STUDY

- Avoid visiting unsecured / unsafe / unknown websites.
- Avoid using unknown browsers.
- Avoid using / saving passwords on public devices
- Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.

- Turn on two-factor authentication where such facility is available.
- Be wary of suspicious looking pop ups that appear during your browsing sessions on internet.
- Always check for a secure payment gateway (https:// - URL with a pad lock symbol) before making online payments / transactions.

1.12 CONCLUSION

The study concludes that, digital banking is significant revolution in banking sector that facilitates high convenience and speed to the customer and cost effective to the banking sector. However, digital banking is subject to high risk of personal information theft by the hackers. Thus, present study revealed that poor customer awareness, sharing of credentials, frequent attempts by the frauds, unsecured technology, wide use of UPI codes, low awareness campaigns are causes of online digital banking. The study suggests that, banks and cyber crime department should be able in finding the bank accounts and take recovery of loss amount and closing of that account based on the complaint of the victims.

1.13 REFERANCES

1.Scratchley, Arthur. 1860. *A Practical Treatise on Savings Banks: Containing a Review of Their Past History and Present Condition and of Legislation on the Subject.* London: Longman, Green, Longman, And Roberts. Accessed December 22, 2020 https://ia800204.us.archive.org/1/items/cu31924014533289/cu31924014533289.pdf.

2.Solanker, V. Rajaram. 1937. *Banking frauds in India.* Bombay: D. B. Taraporevala Sons & Co.

3. Sharma, B.R. 2009. *Bank Fraud: Prevention & Detection.* Third Edition. New Delhi: Universal Law Publishing Co. Pvt Ltd.

4. Nainta, R. P. 2005. *Banking System, Frauds and Legal Control.* New Delhi: Deep & Deep Publications Pvt. Ltd.

5. Sharma, S. and Brahma, A. 2000. "A Role of Insider in Banking Fraud." manupatra.com. Accessed February 4, 2021. https://www.manupatrafast.com/articles/articleSearch.aspx#.

6. FDIC is an independent agency which was created by the United States Federal Government in 1933 under the Banking Act,1933, in the backdrop of multiple bank failures during the 1920-

1930 decade, with a view to provide and maintain stability and public confidence in the nation's financial system. To achieve its objectives, FDIC, insures deposits; examines and supervises financial institutions for safety, soundness, and consumer protection.

7. Federal Deposit Insurance Corporation. n.d. *"Bank Fraud and Insider Abuse, Section 9.1." FDIC: Manual of Examination Policies.* Pg. 2
Accessed October 08, 2020. https://www.fdic.gov/regulations/safety/manual/section9-1.pdf.

8. Association of Certified Fraud Examiners (ACFE). 2018. *Report to The Nations: 2018 Global Study on Occupational Fraud and Abuse.* Association of Certified Fraud Examiners. Accessed June 16, 2020. https://www.acfe.com/report-to-the-nations/2018/default.aspx.

9.Singh, Charan and Pattanayak, Deepanshu and Dixit, Divyesh and Antony, Kiran and Agarwala, Mohit and Kant, Ravi and Mukunda, S and Nayak, Siddharth and Makked, Suryaansh and Singh, Tamanna and Mathur, Vipul. 2016. "Frauds in the Indian Banking Industry." *IIM Bangalore Research Paper No. 505.* March 2. Accessed October 2, 2020. https://www.iimb.ac.in/sites/default/files/2018-07/WP_No._505.pdf.

10.Scratchley, Arthur. 1860. *A Practical Treatise on Savings Banks: Containing a Review of Their Past History and Present Condition and of Legislation on the Subject.* London: Longman, Green, Longman, And Roberts. Accessed December 22, 2020

https://ia800204.us.archive.org/1/items/cu31924014533289/cu31924014533289.pdf.

11. Solanker, V. Rajaram. 1937. *Banking frauds in India*. Bombay: D. B. Taraporevala Sons & Co.

12. Sharma, B.R. 2009. *Bank Fraud: Prevention & Detection.* Third Edition. New Delhi: Universal Law Publishing Co. Pvt Ltd.

DIGITAL BANKING FRAUDS - A CASE STUDY OF TELENGANA

DEMOGRAPHIC PROFILE OF THE BANK CUSTOMERS

1. Name of the customer:
2. Gender of the customer: Male ( ) Female ( )
3. Educational Qualification: SSS ( ) Intermediate ( ) Degree ( ) Post Graduation ( )
4. Region: Rural ( ) Urban ( ) Semi ( ) Metro politon city ( )
5. How many years far you are using online banking
   Less than one yea ( ) 1-2 years ( ) 2-3 Years ( ) 3-4 Years ( ) above 4 years ( )
6. How many years far you are using mobile banking
7. Less than one ye ( ) 1-2 years ( ) 2-3 Years ( ) 3-4 Years ( ) above 4 years ( )
8. Size of transactions you will do in online banking per month
   Less than Rs 10000 ( ) Rs 10001- Rs 100000 ( )
   Rs 100000-Rs 500000 ( ) Above Rs 500000 ( )
9. Form of digital banking frauds you are exposed

Form of fraud	Select the option
ATM card skimming	
QR code scan	
Fake advertisement for loans	
Asking OTP/CVV	
Loans with forged documents	
KYC update calls	
Account blocked messages	
SMS/E-mail	

Others (Please specify	

10. Are you victim of banking frauds Yes ( ) No ( )

If Yes, tell me the amount range you loss

a) ( ) b) Rs 10001-Rs 100000 c) Rs 100001 – Rs 500000 d) above Rs 500000

11. How Did you react immediately after detecting digital banking fraud (Please tick option)

1	Blocking card/online banking/mobile banking services, changing passwords	
2	Complaint to the nearest bank branch	
3	Complaint to the cyber crime	
4	Simply changing pass words, without complaint	
	Total	

12. Is your bank compensated your loss due to digital banking

Fully compensated ( ) partially compensated ( ) No at all compensated ( )

13. Are you satisfied with the actions taken by your bank or cyber crime department against your complaint?

Highly satisfied ( ) Moderately Satisfied ( ) Dissatisfied ( ) Highly Dissatisfied ( )

14. Did you block your online banking facilities after fraud deducted

Yes ( ) No ( )

15: did you reactivate you digital banking facility after experience of digital banking fraud.

Yes ( ) No ( )

16: Please Rate your Experience from using digital banking

Excellent ( ) Good ( ) Poor ( ) Worst ( ) Dangerous ( )

17. What is impact of financial fraud on your financial status

Highly significant ( ) Significant ( ) Moderate ( ) Negligible ( )

18: Please give suggestions for improving the safety of digital banking

_____

FIELD SURVEY AND COLLECTION OF DATA


SBI
Government Degree College
Hayathnagar
Rangareddy Dist., Telangana
(Affiliated to Osmania University)
DEPARTMENT OF COMMERCE
Jignasa Student Study Project
Awareness Program on
Digital Banking Frauds
Dr. Gundeti Somha
Supervisor
Dr.K Jyotsna Prabha
Principal


SDI
BRANCH PERFORMANCE
BRANCH NAME : KUNTLOOR ROAD BRANCH HANDHNAGAR BRANCH CODE: 21096
PARAMETERS
AS ON 31-03-2022
BUDGET
31-10-22 AS ON DATE
GROWTH
DEPOSITS
CASA
ADVANCES
PBBU
REHBU
SMEBU
ABU
NPA
RADAR
PREV SCORE
CRM
ORM
SCORE
CURRENT %


PERSONAL ACCIDENTAL INSURANCE
₹500/= ₹10/-Lacs Cover
₹1000/= ₹20/-Lacs Cover
SBI
NO MEDICAL TEST


Digital Banking frauds
Jignasa Student Study project


Digital Banking Frauds