Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Debit Card and Credit Card Fraud Investigation in Bengaluru City

Mr. Yerriswamy K,

Ph.D.Research Scholar, The Dept. of Studies in Criminology and Forensic ScienceKarnatak University, Dharwad.

Dr. G. S. Venumadhava,

Associate Professor & Chairman, The Dept. of Studies inCriminology and Forensic Science, Karnatak University, Dharwad.

Article Info

Page Number: 3230 - 3247

Publication Issue:

Vol 71 No. 4 (2022)

Abstract

Debit card and Credit card fraud is a type of identity theft that involves the unlawful use of another person's credit card information in order to charge transactions to the account or withdraw funds from it. Debit card fraud happens when a criminal obtains one debit card number (and, in some situations, their personal identification number (PIN)) in order to make unauthorized purchases or withdraw cash from their account. The current study has used secondary data which included 300 Police reported cases of debit/credit card frauds that have been reported in Bengaluru City over the past five years. The collected data have been organized and looked into thoroughly for the details pertain to the crime. The were analysed and interpreted using statistics to find the trends and causes for these crimes. The study has employed both descriptive (frequency and percentage) and inferential statistics (chi-square test) using SPSS for windows. The obtained results were quantitatively interpreted and further qualitatively interpreted with supporting literature.The results revealedthe number of Police reported cases related to Debit card frauds was higher than Credit card frauds and this might be due to the excessive use of debit cards. Males were the frequent victims of financial fraud as women tend to stay away from risks and are slightly careful about their privacy and identity. The Eastern part of Bangalore which is the Information Technology hub (IT hub) of the city was found to have reported the majority of financial fraud cases. Nowadays OTP frauds have become common because of the effortless way to do it. Individuals with private jobs are more prone to financial fraud than students as having a decent salary that is being saved

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

in their accounts is a guarantee for the fraudster. It was found that criminals focused on making quick money with small amounts rather than aiming for larger ones to be safe from being caught or penalized.

Keywords: Reported cases, Privacy,IT hub, Financial fraud, Fraudster

Introduction:

Credit card fraud is a type of identity theft that involves the unlawful use of another person's credit card information in order to charge transactions to the account or withdraw funds from it. Debit card fraud happens when a criminal obtains one debit card number (and, in some situations, their personal identification number (PIN)) in order to make unauthorized purchases or withdraw cash from their account. In today's economic scenario, credit card and Debit card use has skyrocketed. These cards enable users to make large-scale payments without carrying enormous amounts of cash. They have changed the way consumers make cashless payments and have made payments more convenient for purchasers. This electronic payment method is convenient, but it also has a number of drawbacks. Credit card and debit card scams are growing at a similar rate as the number of consumers increases. Credit card and debit card information about a specific person could be obtained fraudulently and used for fraudulent transactions.

Bangalore is one of the largest metropolitan city and the nation's leading information technology (IT) exporter and this becomes the basis for being a hub for such frauds. Studies were conducted on the investigation of card skimming cases as Card fraud is one of the most common types of banking fraud, with card skimming accounting for the largest share. Card skimming investigations and prosecutions rely heavily on digital evidence, which necessitates the use of experienced and skilled law enforcement investigators. Furthermore, a single episode of card skimming results in the acquisition of information from hundreds of cards, making the identification of all victims a significant difficulty for an investigating officer. The paper examined several card skimming difficulties, providing a comprehensive overview of the mode of operation, investigative method, and limits faced by law enforcement authorities (Shetty & Murthy, 2022). However, the study failed to focus on important topics like the causes for skimming and what are the simple ways that individuals could be aware of to avoid such frauds. The paper mainly

concluded with the problems faced for investigation and limits faced by law enforcement authorities rather than explaining their current role and success.

Another study investigated the subject of fraud from the standpoint of the banking business. The study aimed to assess the many factors that contribute to bank fraud. It intended to investigate the extent to which bank personnel adheres to different fraud prevention procedures, including those recommended by the Reserve Bank of India. It attempted to provide insight into bank employees' perceptions of preventive mechanisms and their awareness of various frauds. The study emphasized the significance of training in the prevention of bank fraud. A solid internal control system and good hiring procedures avoid fraud and limit losses. According to their findings, the implementation of various internal control systems is inadequate and, the main causes of bank fraud are a lack of training, overloaded employees, competition, and a low compliance level (the extent to which procedures and prudential standards are defined by the Reserve Bank of India to avoid fraud are followed). Banks must take the rising trend of bank fraud seriously and ensure that internal control mechanisms are not slack (Khanna & Arora, 2009). The study failed to find strong recommendations or methods to avoid such frauds and also focused on problems inside a bank setting rather than external factors.

As mentioned above Banglore is a hub for IT sectors and also called as India’s cybercrime capital, so a study was conducted on IT security management. The beginning of financial deregulation, globalization, and hence the emergence of new technologically sophisticated market competitors with customer-centric business models posed a significant threat to India's public sector banks (PSBs), which have been in the banking business for more than a century. These banks quickly realized that technology-based banking solutions were the only way to stay in business and, as a result, began introducing technology-based solutions at a faster pace, without reforming their information security management at the same rate, exposing themselves to information system-related security threats. In the paper, an investigational study on the preparation and currently widespread IT security management practices of PSBs is presented utilizing a case study research design and techniques. The potential vulnerabilities that exist in the system with specific reference to data leaks and suggestions to safeguard these banks from such threats are presented (Diwakar & Naik, 2008). However, the study investigated the security management and how well it is protected rather than what frauds are taking place. It focused on bank frauds as a whole and failed to be specific about card frauds, skimming, or phishing.

Whereas the current study talks about cybercrime and different types of it the mainly focuses on credit and debit card frauds based in Bangalore and its investigation. The study examines the various challenges faced by police officers and lawyers in debit and credit card related investigations, compares difficulty in investigation between debit and credit cards, and elicits and suggests the technical, investigation measures to prevent the debit and credit card frauds. Present research study also concentrates on the different investigation methods followed by the investigation officer to trace the fraud and techniques utilized to find out the fraud.

Methodology:

The current study has used secondary data which included 300 Police reported cases of credit/debit card frauds that have been reported in Bengaluru City over the past five years. The collected data have been organized and looked into thoroughly for the details pertain to the crime. The were analysed and interpreted using statistics to find the trends and causes for these crimes. The study has employed both descriptive (frequency and percentage) and inferential statistics (chi-square test) using SPSS for windows. The obtained results were quantitatively interpreted and further qualitatively interpreted with supporting literature.

Results: Table 1 shows the Frequency and Percent distribution of Types of credit/Debit card frauds by various demographic variables of victim and chi-square test results

			Type of Card		Total	Test statistics
			Debit	Credit		
Total		F	158	142	300	$X^2_{(O)}$= .853 p= .356
		%	52.7%	47.3%	100.0%	
Gender	Male	F	110	108	218	$X^2_{(A)}$= 1.560 p= .243^{FET}
		%	69.6%	76.1%	72.7%	
	Female	F	48	34	82	$X^2_{(O)}$= 61.653 p= .001
		%	30.4%	23.9%	27.3%	
Age groups	30 and below	F	37	26	63	$X^2_{(A)}$= 2.206 p= .531
		%	23.4%	18.3%	21.0%	
	31-40	F	68	69	137	
		%	43.0%	48.6%	45.7%	
	41-50	F	34	34	68	$X^2_{(O)}$= 78.480 p= .001
		%	21.5%	23.9%	22.7%	
	50+	F	19	13	32	
		%	12.0%	9.2%	10.7%	

Area (in Bengaluru city)	North	F	23	18	41	$X^2_{(A)}$= 10.475 p= .106
		%	14.6%	12.7%	13.7%	
	South	F	36	17	53	
		%	22.8%	12.0%	17.7%	
	East	F	31	29	60	
		%	19.6%	20.4%	20.0%	
	West	F	21	18	39	
		%	13.3%	12.7%	13.0%	
	Central	F	17	27	44	
		%	10.8%	19.0%	14.7%	$X^2_{(O)}$= 17.707 p= .007
	South East	F	16	22	38	
		%	10.1%	15.5%	12.7%	
	North East	F	14	11	25	
		%	8.9%	7.7%	8.3%	
Occupation	Govt	F	27	25	52	
		%	17.1%	17.6%	17.3%	
	Private	F	105	105	210	$X^2_{(A)}$= 9.112 p= .028
		%	66.5%	73.9%	70.0%	
	Business	F	17	12	29	
		%	10.8%	8.5%	9.7%	$X^2_{(O)}$= 336.34 p= .001
	Student	F	9	0	9	
		%	5.7%	0.0%	3.0%	

Gender - It was seen that 72.7% of the victims were male while 27.3% of them were female. The chi square test revealed a significant difference (X^2=61.653; p=.001) indicating that a majority of the victims were male. Furthermore, the chi-square test for the association between gender and type of card fraud showed a non-significant association (X^2=1.560; p=.243) indicating that type of card fraud are similar in both genders.

Age group - There were 45.7% of the victims who belonged to the age group 31-40, while 22.7% belonged to the age group 41-50, 21.0% of the victims belonged to 30 & below and 10.7% of the victims belonged to the age group 50+. The chi-square test showed a significant difference (X^2=78.480; p=.001) which elucidates that a greater number of the victims are of the age group 31-40. However the chi-square test for the association between age group and type of card fraud revealed a non-significant association (X^2=2.206; p=.531) elucidating that all age groups experienced both type of card fraud.

Area in Bengaluru city - Out of the victims, it was observed that 20.0% of them were from Bengaluru east, 17.7% were from Bengaluru south, 14.7% of them were of the Bengaluru central

area, while 13.7% were from north Bengaluru, 13.0% of the victims were from Bengaluru west, 12.7% were from south-east Bengaluru and 8.3% were from north-east Bengaluru. The chi-square test revealed a significant difference (X^2=17.707; p=.007) which indicates that a higher number of victims were from Bengaluru east. Moreover, the chi-square test for the association between area and type of card fraud showed a non-significant association (X^2=10.475; p=.106) elucidating that victims of different areas experienced both types of card fraud.

Occupation - It was observed that 70.0% of the victims worked in the private sector, 17.3% worked in the government sector, while 9.7% had their own business and 3.0% of the victims were students. The chi-square test revealed a significant difference (336.34; p=.001) elucidating that a majority of the victims work in the private sector. Furthermore, the chi-square test for the association between occupation and type of card fraud revealed a significant association (X^2=9.112; p=.028) indicating that a higher number of victims working in private and government sector experienced Credit card fraud while a greater number of victims having their own business and students experienced Debit card fraud.

Table 2 shows the Frequency and Percent distribution of Types of credit/Debit card frauds by Crime details and chi-square test results

			Type of Card		Total	Test statistics
			Debit	Credit		
Causes of Cybercrime	Recognition	F	4	5	9	$X^2_{(A)}$= .252 p= .740
		%	2.5%	3.5%	3.0%	
	Quick money	F	154	137	291	$X^2_{(O)}$= 265.080 p= .001
		%	97.5%	96.5%	97.0%	
Type of crime	Person	F	152	139	291	$X^2_{(A)}$= .729 p= .507
		%	96.2%	97.9%	97.0%	
	Property	F	6	3	9	$X^2_{(O)}$= 256.080 p= .001
		%	3.8%	2.1%	3.0%	
Type of Card fraud	Account taken over	F	24	18	42	$X^2_{(A)}$= 11.251 p= .081
		%	15.2%	12.7%	14.0%	
	OTP fraud	F	85	89	174	
		%	53.8%	62.7%	58.0%	
	Application fraud	F	4	0	4	$X^2_{(O)}$= 572.807 p= .001
		%	2.5%	0.0%	1.3%	
	Fake card	F	38	35	73	
		%	24.1%	24.6%	24.3%	

	Lost/stolen card	F	4	0	4	
		%	2.5%	0.0%	1.3%	
	Website cloning	F	2	0	2	
		%	1.3%	0.0%	0.7%	
	Skimming	F	1	0	1	
		%	0.6%	0.0%	0.3%	
Amount lost (in rupees)	Below 50,000	F	113	107	220	$X^2_{(A)}$= .562 p= .514^{FET}
		%	71.5%	75.4%	73.3%	
	Above 50,000	F	45	35	80	$X^2_{(O)}$= 65.33 p= .001
		%	28.5%	24.6%	26.7%	
Bank status	Non Nationalized	F	67	53	120	$X^2_{(A)}$= .805 p= .409 ^{FET}
		%	42.4%	37.3%	40.0%	
	Nationalized	F	91	89	180	$X^2_{(O)}$= 12.00 p= .001
		%	57.6%	62.7%	60.0%	
Loop holes	Details shared	F	108	87	195	$X^2_{(A)}$= 10.090 p= .006
		%	68.4%	61.3%	65.0%	
	Bank fault	F	29	46	75	$X^2_{(O)}$= 145.50 p= .001
		%	18.4%	32.4%	25.0%	
	Both	F	21	9	30	
		%	13.3%	6.3%	10.0%	

Causes of cybercrime - It was seen that 97.0% of cybercrime was caused for Quick money while 3.0% were caused for recognition. The chi-square test revealed a significant difference (X^2=265.080; p=.001) which indicates that a greater number of cyber-crime were caused for quick money. Moreover, the chi-square test for the association between cause of cybercrime and type of card fraud showed a non-significant association (X^2=.252; p=.740) elucidating that causes of cybercrimes were not associated with the type of card fraud.

Type of crime - On the type of crime, it was seen that 97.0% of the crimes were against a person while 3.0% were against a person's property. The chi-square test revealed a significant difference (X^2=256.080; p=.001) indicating that a higher number of crimes were against a person. However, the chi-square test for the association between type of crime and type of card fraud showed a non-significant association (X^2=.729; p=.507) elucidating that both card frauds were experienced in both types of crime.

Type of Fraud - There were 58.0% of OTP fraud, 24.3% of the frauds were fake card, 14.0% were account taken over, 1.3% were application fraud as well as lost/stolen card, while 0.7% were

website cloning and 0.3% were skimming. The chi-square test revealed a significant difference (X^2=572.807; p=.001) indicating that a majority of the fraud were OTP fraud. Moreover, the chi-square test for the association between type of fraud and type of card fraud showed a non-significant association (X^2=11.251; p=.081) which indicates that type of fraud is similar in victims of both types of card fraud.

Amount lost - It was seen that 73.3% of victims lost amount below 50,000 rupees, while 26.7% of them lost above 50,000 rupees. The chi-square test revealed a significant difference (X^2=65.33; p=.001) which elucidates that a majority of the victims lost amounts below 50,000 rupees. In addition, the chi-square test for association between amount lost and type of card fraud showed a non-significant association (X^2=.562; p=.514) elucidating that type of card fraud is similar of victims who lost above and below 50,000 rupees.

Bank status - It was observed that 60.0% of victims' bank were Nationalised while 40.0% of them were non-nationalised. The chi-square test revealed a significant difference (X^2=12.00; p=.001) indicating that a higher number of the victims' bank are Nationalized. The chi-square test for the association between bank status and type of card fraud showed a non-significant association (X^2=.805; p=.409) which indicates that type of card fraud is similar in both types of banks.

Loopholes - It was seen that 65.0% of the loopholes were from details shared by the victim while 25.0% of them were bank fault and 10.0% were both. The chi-square test revealed a significant difference (X^2=145.50; p=.001) which indicates that a greater number of loopholes were from the details shared by the victim. Furthermore, the chi-square test for the association between loopholes and typed of card fraud revealed a significant association (X^2=10.090; p=.006) elucidating that majority of the loopholes from details shared by the victim were of debit card fraud while a higher number of loopholes from bank fault were of credit card frauds.

Table 3 shows the Frequency and Percent distribution of Types of credit/Debit card frauds by Investigation procedure and chi-square test results

			Type of Card		Total	Test statistics
			Debit	Credit		
Investigation outcome	Evidence found	F	156	137	293	$X^2_{(A)}$= 1.669 p= .262 FET
		%	98.7%	96.5%	97.7%	
	Evidence	F	2	5	7	

	not found	%	1.3%	3.5%	2.3%	$X^2_{(O)}$= 272.653 p= .001
Investigation mode	Offline	F	4	3	7	$X^2_{(A)}$= .058 p= 1.00 FET
		%	2.5%	2.1%	2.3%	
	Online	F	154	139	293	$X^2_{(O)}$= 272.653 p= .001
		%	97.5%	97.9%	97.7%	
Time taken by Victim to report to the Cyber crime station	<12 hr	F	16	25	41	$X^2_{(A)}$= 5.729 p= .220
		%	10.1%	17.6%	13.7%	
	13-24 hr	F	20	11	31	
		%	12.7%	7.7%	10.3%	
	25-48 hr	F	49	41	90	
		%	31.0%	28.9%	30.0%	
	49-72 hr	F	23	16	39	$X^2_{(O)}$= 67.733 p= .001
		%	14.6%	11.3%	13.0%	
	above 72 hr	F	50	49	99	
		%	31.6%	34.5%	33.0%	
Complaint given in	Oral	F	0	4	4	$X^2_{(A)}$= 4.511 p= .049 FET
		%	0.0%	2.8%	1.3%	
	Written	F	158	138	296	$X^2_{(O)}$= 284.213 p= .001
		%	100.0%	97.2%	98.7%	
Crime duration in hours	0-6 h	F	91	88	179	$X^2_{(A)}$= 5.275 p= .153
		%	57.6%	62.0%	59.7%	
	6.01-12 hr	F	47	29	76	
		%	29.7%	20.4%	25.3%	
	12.01-18 hr	F	14	21	35	$X^2_{(O)}$= 221.893 p= .001
		%	8.9%	14.8%	11.7%	
	18.01-24 hr	F	6	4	10	
		%	3.8%	2.8%	3.3%	
Did the victim know the criminal ?	Known	F	2	2	4	$X^2_{(A)}$= .012 p= 1.00 FET
		%	1.3%	1.4%	1.3%	
	Unknown	F	156	140	296	$X^2_{(O)}$= 284.213 p= .001
		%	98.7%	98.6%	98.7%	
Gender of the criminal	Male	F	142	130	272	$X^2_{(A)}$= .248 p= .693 FET
		%	89.9%	91.5%	90.7%	
	Female	F	16	12	28	$X^2_{(O)}$= 198.453 p= .001
		%	10.1%	8.5%	9.3%	

Investigation outcome - On investigation outcome, it was observed that in 97.7% of the cases evidence was found while in 2.3% of the cases evidence was not found. The chi-square test revealed

a significant difference (X^2=272.653; p=.001) elucidating that evidence was found in majority of the cases. In addition, the chi-square test for the association between investigation outcome and type of card fraud showed a non-significant association (X^2=1.669; p=.262) which elucidates that investigation outcome was similar in both types of card fraud.

Investigation mode - It was observed that 97.7% of the cases were investigated Online while 2.3% of the cases were investigated Offline. The chi-square test revealed a significant difference (X^2=272.65; p=.001) indicating that a greater number of the cases were investigated Online. Moreover, the chi-square test for the association between investigation mode and type of card fraud showed a non-significant association (X^2=.058; p=1.00) indicating that in both types of card frauds the investigation mode was similar.

Time taken by the victim to report to the cyber crime station - On time take by the victim to report to the cyber crime station, 33.0% of the victims took above 72 hr, 30.0% of them took 25-48 hr, 13.7% of the victims took less that 12 hr, while 13.0% took 49-72 grand 10.3% of the victims took 13-24 hr. The chi-square test showed a significant difference (X^2=67.733; p=.001) which elucidates that a greater number of victims reported after 72hr. In addition, the chi-square test for the association between the time take to report to cyber crime station and type of card fraud showed a non-significant association (X^2=5.729; p=.220) indicating that time taken by the victims is similar in both types of card frauds

Complaint given in - It was seen that 98.7% of the victims gave the complaint in written while 1.3% of the victims gave the complaint orally. The chi-square test showed a significant difference (X^2=284.213; p=.001) elucidating that majority of the victims gave the complaint in written format. Furthermore, the ci-square test for the association between complaint given in and type of card fraud showed a significant association (X^2= 4.511; p=.049) which elucidates that higher number victims of debit card fraud gave complaint in written while a greater number of victims of credit card fraud gave the complaint orally.

Crime duration - It was observed that 59.7% of the crimes took 0-6 hr, while 25.3% of them took 6.01-12 hr, 11.7% of them took 12.01-18hr and 3.3% of the crime took 18.01-24 hr. The chi-square test showed a significant difference (X^2=221.893; p=.001) indicating that a higher number of crimes took 0-6 hr. In addition, the chi-square test for the association between crime duration and type of

card fraud revealed a non-significant association (X^2=5.275; p=.153) elucidating that crime duration was similar in both types of card frauds.

Did the victim know the criminal - It was seen that in 98.7% of the cases the victim did not know the criminal, while 1.3% of the victims knew the criminal. The chi-square test showed a significant difference (X^2=284.213; p=.001) which indicates that the majority of victims did not know the criminal. Moreover, the chi-square test for the association between victim knowing the criminal and type of card fraud showed a non-significant association (X^2=.012; p=1.00) elucidating that in both types of card frauds the victim knowing and not knowing the criminal was similar.

Gender of the criminal - 90.7% of the criminals were male , while 9.3% of them were female. The chi-square test revealed a significant difference (X^2=198.453; p=.001) indicating that a greater number of the criminals were male. Furthermore, the chi-square test for the association between gender of the criminal and types of card fraud showed a non-significant association (X^2=.248; p=.693) which indicates that both male and female criminals frauded victims in both types of card frauds

Major findings of the study:

- A total of 300 Police reported cases were analyzed, of them, 52.7% of the Police reported cases were related to debit card frauds and 47.3% of the Police reported cases were related to credit card frauds.
- Majority of the fraud victims were males to an extent of 72.7% and remaining 27.3% of them were females.
- Police reported cases revealed that individuals in the age group of 31-40 years were affected more (45.7%), whereas individuals in the age group of 50 and above years were affected less (10.7%), and others in between.
- From the FIR, it was revealed that 20% of the cases were reported in East part of Bengaluru city, whereas, the least was observed in North east (8.3%) of Bengaluru city.
- All the Victims of the Credit/Debit card frauds were Indians.
- 70% of the Victims had Private Jobs while there were 3% of the students who had experienced Credit/Debit card frauds.
- Half of the FIR's reported were victims using SBI while the other half was composed by other banks such as City bank, Kar Bank, Axis Bank and many others.

- Police reported cases showed that 97% of the crimes were caused due to quick money and were done against person.
- Majority of 58% if the card frauds were OTP frauds, followed by 24.3% of the Police reported cases reported were Fake card frauds.
- 73.3% of the Police reported cases reported that amount lost was below 50,000 rupees while the remaining were above 50,000 rupees.
- 65% of the crimes had occurred due to the details shared by the Victim, however there were 25% of the crimes which were due to Bank's fault and 10% included both's fault. Further, 32.4% of the credit card frauds were due to bank faults.
- 97.7% of the crime's Evidence were found and it was also found that 97.7% of the Investigation was done Online.
- It was observed that 33% of the victims took more than 72 hours to report to the Cyber crime station, 30% of them took 25-48 hours and only 13.7% reported before 12 hours of the cybercrime.
- It was evident that 98.7% of the complaints were given in written.
- FIR's revealed that crimes were done between 0-6 hours while only 3.3% of the crimes took 18-24 hours.
- 98.7% of the FIR's reported that the criminals were unknown to the victim. Further, it was also observed 90.7% of the criminals were males.

From the study, it was revealed that in about 300 Police reported cases filed, about 57.7% were debit card frauds and 47.3%. When an individual opens a savings account, he/she immediately gets a debit card, this is how easily a debit card can be claimed but to own a credit card, is a lengthier and slightly more complicated process (Truong, et.al, 2020). So due to such reasons, the population of people owning a debit card seems to be larger than the population owning a credit card and this might be one inference on why there are more debit card frauds than debit card frauds. Also if a credit card is stolen, there is zero liability for customers and they are not reported for fraudulent charges either so the responsibility is taken up (Burns & Stanley, 2002). The study found that the majority of victims were men with 72.2% and women were just a mere 27.3%. Copes, et.al, 2010 conducted a study and in their survey, it was found that women report more identity theft than men but also that they are more protective and careful of their financial information than men. Once

women experience identity theft, they tend to go and find ways to be careful and make sure that they do not fall into such traps again. A study revealed that 73% of males in India who proceeded to interact with a scammer were likely to lose money (Steffensmeier, et.al, 2013). This might be considered as to why men were the majority victims of fraud. The study revealed that individuals in the age groups of 31-40 were affected more than the individuals in the age group of 50 and above. This conclusion might be made because some studies show that older people are mostly not aware of what these frauds are and how much of their money is lost, it is either some younger family member who detects it or reports it (Temple, 2007). In India, millennials (aged between 24 and 37) were the most susceptible to such scams in 2021, with 58% of those that continued with the scam incurring a monetary loss. In the study, it was revealed that 20% of the cases were reported in the East part of Bengaluru city, whereas, the least was observed in the Northeast (8.3%) of Bengaluru city. The east of Bangalore includes areas like Marathahalli and Sarjapur which are IT hubs, therefore people leaving here are individuals working for reputed companies and earn a decent good salary, whereas areas in Bangalore northeast are industrial areas, medical, engineering colleges, and individuals leaving here are either students or daily wage laborers at factories who tend have lesser money in their accounts and also would not have a fast-paced life (Sánchez, et.al, 2009). All the Victims of the Credit/Debit card frauds were Indians. India was ranked among the top five countries globally that are vulnerable to credit card fraud, according to the 2016 Global Consumer Fraud Report. This might be because of the lack of awareness in people about the usage of cards and knowing about their privacy of it. Govindarajan, et.al 2012 conducted a study on the utilization and awareness of credit cards and here it was set out that in India, people from smaller cities apply for debit cards or credit cards without fully being aware of the banking transactions and their safety, making them a perfect targets for fraudsters.

70% of the Victims had Private Jobs while there were 3% of the students had experienced Credit/Debit card fraud. One of the main reasons for this finding is that students rarely own a debit/credit card and even if they do it is either someone's in their family or just a debit card with a minimum amount of balance in it. Whereas individuals with private jobs earn good salaries and normally own credit/debit cards of their own and also have a decent amount of money in their accounts, making them the target of fraud (Vahdati & Yasini 2015).

Half of the Police reported cases reported were victims using SBI while the other half was composed of other banks such as City bank, Kar Bank, Axis Bank, and many others. State Bank of India is the largest public sector lender and has the majority of users compared to other banks (Bihari & Mohaptra 2010). As the users of SBI are in majority it is obvious that the frauds are much more prevalent in it. Police reported cases showed that 97% of the crimes were caused due to quick money and were done against the person. The common aim of financial fraud is to make money and ransack as much money as possible. Though financial frauds can be committed with several other motives, quick money-making is the common and most go-to motive (Adediran & Olugbenga 2010). Even if the fraud was committed for a different motive, here it is beneficial because the fraudster is earning a good amount of money and has also gone against the person. The majority of 58% of the card frauds were OTP frauds, followed by 24.3% of the Police reported cases reported were Fake card frauds. As the ease of doing online transactions increased, so did the frequency of frauds in digital financial transactions. Fraudsters are more inventive in their tactics of defrauding individuals (Sankhwar & Pandey 2016). Kulat, et.al, 2016, in their study explained what exactly is an OTP scam and it goes like this, a frequent OTP scam involves the scammer calling a person and posing as someone interested in your goods or service. They agree to pay a specified amount as immediate confirmation, followed by a request for payment gateway or digital wallet information and the OTP. Once the fraudster has gained access to your account, they can carry out a variety of transactions to empty you. This is how easy the process is. The fraudster just needs to let the victim say the 6 or 4-digit OTP that comes on their phone and then done, they get the entire data they wish to access. The rest of the percentage showed fake card fraud which are are comparatively complicated to administer. Therefore the OTP frauds are in majority.

73.3% of the Police reported cases reported that the amount lost was below 50,000 rupees while the remaining were above 50,000 rupees. Every fraud case can be taken up to courts and then get back the lost amount, but the process and the charge for regaining the money back will itself exceed more than 50,000 and that is one main reason why victims who lost below 50,000 tend to ultimately let it go and thus this becomes an advantage for fraudsters and they repeatedly aim for small amounts and make a profit through it. A case in Delhi's Burari area talked about a man who lost Rs 50,000 through his PhonePe wallet and he filed a complaint in the nearby police station this incident took place 2 years back and there seems to be no sign of him getting his money back even after repeated visits to courts and the police station. This is an example of how there is a complex process to claim

the money back and people tend to rather let it go. 65% of the crimes had occurred due to the details shared by the Victim, however, there 25% of the crimes were due to Bank's fault and 10% included both's fault. Further, 32.4% of the credit card frauds were due to bank faults. OTP frauds are an example of the crimes that occurred due to details shared by the victim. Victims of financial fraud end up sharing much more sensitive information like card details, CVV, bank account numbers, etc and this is because of the lack of awareness about one's privacy and data (Smith & Budd 2009). Khanna & Arora, 2009 conducted a study and according to their findings, the main causes of bank fraud are a lack of training, overloaded employees, competition, and a low compliance level (the extent to which procedures and prudential standards are defined by the Reserve Bank of India to combat fraud are followed). Banks must take the rising trend of bank fraud seriously and ensure that internal control mechanisms are not lax.

97.7% of the crime's Evidence was found and it was also found that 97.7% of the investigation was done Online. Consumers in India experienced a fairly high online fraud encounter rate of 69% in the past year, according to the Microsoft 2021 Global Tech Support Scam Research report. Button, et.al, 2014 in their study claimed that fraud is a fact of life for those doing business online. And gave two reasons why frauds are sp prevalent online and they are stolen credit card information is easy to buy and prosecution is rare, and online fraud may be a low priority for law enforcement, due to difficulty amassing evidence and time and resource constraints. Ecommerce fraud may be regarded as a low-priority offense. A single instance of fraud may result in a small monetary amount. It is frequently difficult to identify a victim. Legitimate cardholders are often paid for their losses by their issuing bank, which reduces the incentive to pursue a case (Agarwal & Bansal), So it's clear that when most frauds are done online, the available fraud is sure to be found online. It was observed that 33% of the victims took more than 72 hours to report to the Cybercrime station, 30% of them took 25-48 hours and only 13.7% reported before 12 hours of the cybercrime. Police reported casestly, for people to find out that they have been a victim of these frauds itself consumes much time. Then it's a battle for them to decide between if filing a complaint is important or not. Kerley and Copes 2002 in their study discussed victims are fraud are hesitant to report crimes because of the fear of being judged or shamed by society. And some also assume that the procedure for all of it will be complex and are not aware of how they work. But again only 33% do not report it immediately and the rest 30% and 13% report it to the cybercrime police station within 25-48 hours and 12 hours of the crime respectively. It was evident that 98.7% of the complaints were

given in writing. The procedure for filing a cybercrime complaint is Police reported casest writing it down and then submitting it to the police for them to file the FIR (Bidgoli, et.al, 2019). Frauds like fake cards, OTP frauds, and UPI frauds require details like the account holder's name, number, bank details, etc, and these are preferred to be written down than orally said as they are important details that are needed for further investigation.

Police reported cases revealed that crimes were done between 0-6 hours while only 3.3% of the crimes took 18-24 hours. The majority of crimes are done within 6 hours because of how effortless they have become. Online OTP frauds, phishing, SMS scams, etc are called the fast money-making frauds for brisk they are to be completed (Gottlober, 1953). OTP frauds are indeed the easiest as they need the individual to mention the 6 or 4-digit OTP that's sent to their phones and once that is shared the fraudster can get access to what he/she needs. 98.7% of the Police reported cases reported that the criminals were unknown to the victim. Further, it was also observed that 90.7% of the criminals were males. Fraudsters commonly target people whom they are strangers because it's less risky. They mostly need to call these victims, so the fear of being recognized is one reason. For example, if fraud is done on a known person, the police officials Police reported casestly do target the victim's friends and family (Kenny, 2020). It is found that 90.7% of the criminals were males. From a global survey, approximately 73 percent of all fraudsters in the reported cases were male in 2020 and 2021 (Kaatz, et.al, 2013). Steffensmeier, et.al, 2013, in their study believed that female executives may improve ethical standards, or the findings suggested that women generally take fewer risks and self-censor more due to feeling they are under greater surveillance than males colleagues. In addition, women may not have as much access in the financial world and so 1ess opportunity to profiteer.

Conclusions:

The number of Police reported cases related to Debit card frauds was higher than Credit card frauds and this might be due to the excessive use of debit cards. Males were the frequent victims of financial fraud as women tend to stay away from risks and are slightly careful about their privacy and identity. The Eastern part of Bangalore which is the IT hub of the city was found to have reported the majority of financial fraud cases. Nowadays OTP frauds have become common because of the effortless way to do it. Individuals with private jobs are more prone to financial fraud than students as having a decent salary that is being saved in their accounts is a guarantee for the

fraudster. It was found that criminals focused on making quick money with small amounts rather than aiming for larger ones to be safe from being caught or penalized. The majority of financial frauds were done online to hide identity and also as it was turning out to be an accessible portal for money-making. Also, the majority of the crimes were committed by males.

If obvious trends are accessible based on the current state of both physically and technologically, this study will be valuable for future investigation. It can avoid more debit and credit card frauds if specialists recommend problem-solving solutions based on thorough study, and the findings of the research are implemented to prevent various sorts of card frauds.

References

1. Adediran, S., & Olugbenga, A. K. (2010). Impact of frauds on banks' performance in Nigeria. In The Nigerian Academic Forum (Vol. 19, No. 1, pp. 1-5).
2. Agarwal, C., & Bansal, U. Online Business Frauds: A Case Study of an Online Fraud Survey Company.
3. Bidgoli, M., Knijnenburg, B. P., Grossklags, J., & Wardman, B. (2019, November). Report now. Report effectively. Conceptualizing the industry practice for cybercrime reporting. In 2019 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-10). IEEE.
4. Bihari, S. C., & Mohaptra, R. (2010). An Analysis of the Shortcomings of Banking Industry Technology Leading to Default & Fraud With Special Focus on State Bank of India. i-Manager's Journal on Management, 4(4), 70.
5. Burns, P., & Stanley, A. (2002). Fraud management in the credit card industry. Federal Reserve Bank of Philla Payment Cards Center Discussion Paper, (02-05).
6. Diwakar, H., & Naik, A. (2008, July). Investigation of Information Security Management Practices in Indian Pubic Sector Banks. In *2008 IEEE 8th International Conference on Computer and Information Technology Workshops* (pp. 276-281). IEEE.
7. Gottlober, A. B. (1953). Fakers, frauds and fourflushers.
8. Kaatz, A., Vogelman, P. N., & Carnes, M. (2013). Are men more likely than women to commit scientific misconduct? Maybe, maybe not. Mbio, 4(2), e00156-13.

9. Khanna, A., & Arora, B. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry. *International Journal of Business Science & Applied Management (IJBSAM)*, *4*(3), 1-21.
10. Kulat, A., Kulkarni, R., Bhagwat, N., Desai, K., & Kulkarni, M. P. (2016). Prevention of online transaction frauds using OTP generation based on dual layer security mechanism. Int. Res. J. Eng. Technol.(IRJET), 3(4), 1058-1060.
11. Sánchez, D., Vila, M. A., Cerda, L., & Serrano, J. M. (2009). Association rules applied to credit card fraud detection. Expert systems with applications, 36(2), 3630-3640.
12. Sankhwar, S., & Pandey, D. (2016, February). A safeguard against ATM fraud. In 2016 IEEE 6th International Conference on Advanced Computing (IACC) (pp. 701-705). IEEE.
13. Shetty, A. A., & Murthy, K. V. (2022). Investigation of Card Skimming Cases: An Indian Perspective. *Journal of Applied Security Research*, 1-14.
14. Steffensmeier, D. J., Schwartz, J., & Roche, M. (2013). Gender and twenty-Police reported casest-century corporate crime: Female involvement and the gender gap in Enron-era corporate frauds. American Sociological Review, 78(3), 448-476.
15. Steffensmeier, D. J., Schwartz, J., & Roche, M. (2013). Gender and twenty-Police reported casest-century corporate crime: Female involvement and the gender gap in Enron-era corporate frauds. American Sociological Review, 78(3), 448-476.
16. Temple, J. (2007). Older people and credit card fraud. Trends and Issues in Crime and Criminal Justice, (343), 1-6.
17. Truong, T., Phan, H., & Tran, M. (2020). A study on customer satisfaction on debit cards: The case of Vietnam. Uncertain Supply Chain Management, 8(2), 241-251.
18. Vahdati, S., & Yasini, N. (2015). Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. Computers in Human Behavior, 51, 180-187.