ORIGINAL RESEARCH PAPER

Volume - 12 | Issue - 08 | August - 2023 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr

INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

AN EXPLORATIVE STUDY ON BANK FRAUDS IN INDIA.

Management

Braja Kishore Mishra Scholar, Sri Sri University.

Prof. Sunil Kumar Dhal PhD, Sri Sri University

Prof. Subash Nath. PhD, Sri Sri University.

ABSTRACT

Indian economy is mainly dependent on the banking sector. This sector mostly cares for the growth of individuals, groups and organisations; the economy primarily depends on this. For a decade, this sector has been struggling with acts like misappropriation, fraud and financial crime, which all have a bearing on the economy. In this study, I have focussed more on the genesis of fraud. Again, more effort is being made to identify the types of fraud and its financial implication. The analysis of Corporate, Retail, Cyber and Government fraud in India is based on data from reliable sources like RBI Reports, National Crime Bureau and many more. Against this backdrop, a thorough analysis has been made of the sector-wise financial losses by the banks and government.

KEYWORDS

Fraud, Corporate Fraud, Cyber Security, Government Fraud.

INTRODUCTION

Money drives the economy in the digital age, and people often pursue wealth. However, maximal enjoyment and borrowing have replaced saving and reducing expenses. "Live happily and take debt" has become the norm, ignoring the risks of excessive borrowing. Unfortunately, some people have committed fraud to get rich. Fraud, described as "wrongful or criminal deception intended to result in financial or personal gain," is cancer that damages the economy and banking industry. Fraud continues despite efforts to prevent it. Deception destroys confidence and integrity in society. Fraud must be acknowledged and prevented. Fraud can harm individuals, institutions, and society. Ethical behaviour and tight laws can help create a more transparent and trustworthy financial system. It hurts the economy and public trust. Fraudsters hurt financial institutions and innocent individuals. Fraud impairs everyone in society. Due to the massive sums of money and complexity of financial operations, banks are particularly prone to fraud. Banks must protect their interactions with individuals and huge organisations. Fraudsters are constantly finding new ways to defraud banks. Banks must be proactive to prevent fraud. They need robust fraud detection and prevention systems. They must also teach clients how to avoid fraud. Fraud should be punished and deterred by strict legislation. Fraud harms society and the economy. Everyone should know about fraud and prevent it. The banking sector must engage with other stakeholders to combat fraud and protect the financial system. Fraud causes must also be addressed. Fraudsters are often financially destitute or feel victimised by the system. Thus, poverty, inequality, and corruption, which can foster fraud, must be addressed. Technology has also fuelled fraud. Fraudsters are using digital transactions more and more. Thus, banks and other financial institutions must keep up with technology and prevent fraud. Finally, prevention is better than treatment. Financial organisations should avoid fraud rather than discover and penalise it. Education, awareness, and technology can do this. Together, we can build a more secure financial system. Fraud requires a solid legal framework. Clear, strict regulations and serious consequences should deter fraud. This will prevent fraud and hold fraudsters accountable.

Financial institutions must also be honest and transparent. They should be ethical and do the right thing even when it's hard or controversial. They should also be upfront with customers and stakeholders and eager to admit and fix mistakes. Fraud prevention requires cooperation. Financial institutions should collaborate with law enforcement, regulators, and other stakeholders to exchange information, best practices, and fraud prevention and detection measures. Finally, fraud affects more than banks. It impacts healthcare, education, and governance. All parties must collaborate to solve this problem and build a safer, more trustworthy society.

BACKGROUND

According to the Fraud (FraudCircleModel-Fig-1)Circle concept, fraud is caused by various variables that foster fraudulent behaviour. The model links opportunity, weakness, relationship management, and pressure. fraud. Fig-1 (Fraud Circle Model) An organisation's internal control system's vulnerability or weakness can be exploited by a fraudster. Lack of oversight, training, or communication could cause this. A lack of internal controls, rules, or processes makes an individual or organisation vulnerable to fraud. Resources, risk management, and governance may be to blame. Relationship management involves building and maintaining connections with consumers, suppliers, and employees due to a lack of trust, communication, or transparency. Financial concerns, emotional issues, or a desire for power or status might motivate a person or organisation to commit fraud.Fig-1 (Fraud Circle Model)These four characteristics help organisations lower fraud risk. Examples include strengthening internal controls, risk management, transparency, and staff training and assistance. The Fraud Circle paradigm applies to financial, cyber, and identity theft fraud. For financial fraud, the opportunity is a hole in the accounting system that allows an individual to modify financial records, and the pressure is a desire for money to cover personal needs. In cyber fraud, the opportunity is a vulnerability in the organisation's IT system that permits unauthorised access to critical information, and the pressure is retribution or financial gain. Identity theft may be motivated by a hunger for money or power and a hole in the organisation's data security system.

The Fraud Circle model emphasises the significance of an ethical and transparent organisational culture. Organisations can decrease fraud and encourage employees to report suspicious activity by fostering integrity. The Fraud Circle model helps explain fraud's complexity and causes. Organisations can reduce fraud and financial losses by addressing these elements. The concept emphasises constant monitoring and evaluation of internal controls and risk management systems. Organisations can avoid fraud and keep ahead of dangers by reviewing and updating these practices. The Fraud Circle model helps explain fraud's complexity and causes. Organisations can decrease fraud and financial losses by addressing these elements and encouraging integrity.

The Fraud Circle model can also spot fraud warning indications. For instance, a financially stressed person with access to sensitive financial data may conduct fraud. Fraud may also be more prevalent among people with a history of unethical behaviours or poor work relationships. Companies can prevent fraud by detecting these warning indicators. Additional controls, background checks, and ethics training and support may be needed. The Fraud Circle approach emphasises departmental cooperation and communication. Departments can identify and address internal control system deficiencies by exchanging information and working together. The paradigm emphasises external oversight and regulation. By following industry standards, organisations can decrease fraud and avoid legal and financial consequences. The Fraud Circle model helps explain the complexity of fraud and its causes. Addressing these variables and fostering integrity can reduce fraud risk and protect organisations from financial losses and reputational damage.

Fraudsters' strategies: Fraudsters utilise many strategies to defraud others for profit. Misrepresentation, forgery, impersonation, and manipulation can be used. Fraudsters use these methods to steal money, property, and other valuables. Phishing, identity theft, Ponzi schemes, and pyramid schemes are fraud strategies. Know these tricks and take precautions to avoid fraud.

Fraud Types

Account Theft

Account takeover fraud occurs when a criminal hijacks a victim's bank, credit card, or social media account. The offender can then use the account to commit fraud or steal personal information. Criminals can access victims' statements in many ways. Phishing scams include criminals sending emails or texts that look to be from a genuine firm or organisation, requesting the victim to click on a link and input their login credentials. After the victim inputs their details, the criminal can access their account. Malware on the victim's device can steal login passwords and other sensitive data. Account takeover fraud is hard to detect since the criminal may legitimately update or use the account information. Strong passwords, two-factor authentication, and account monitoring for unusual behaviour can help people and corporations avoid this form of fraud. According to the Reserve Bank of India (RBI), bank fraud has increased significantly recently. Banks recorded 8,707 fraud cases worth Rs 1.85 lakh crore in 2019-20. The RBI report does not include data on account takeover frauds, but it underlines fraudsters' growing skills and the need for banks to improve security. In 2020, the Indian Computer Emergency Response Team (CERT-In) recognised account takeover as a top cyber threat to the banking industry. The report warned that thieves use phishing, social engineering, and malware to access bank accounts and steal money. Account takeover fraud is a significant concern to the Indian banking industry, and banks must take precautions to secure their customers' accounts.

Credential Stuffing

Cyber-attackers employ automated software to try multiple stolen usernames and passwords on different websites and apps in the credential stuffing. This exploit steals financial and personal data from user accounts. Data breaches, phishing, and malware infestations give attackers stolen passwords. They then use automated programmes to test these credentials on numerous websites and applications, hoping that some users have reused their usernames and password. Credential stuffing attacks succeed because many users repeat passwords across accounts. Brute force attacks use several usernames and passwords to locate a match. Use strong, unique passwords for each account to prevent credentials stuffing attempts. Multi-factor authentication and rate restriction help prevent automated assaults on websites and apps. Credential stuffing is a severe online security concern that can harm individuals and organisations financially and reputationally. This type of assault requires proactive protection from users and enterprises.

Social Engineering

In social engineering, attackers utilise psychological manipulation to deceive victims into disclosing sensitive information or taking harmful acts. Social engineering exploits human vulnerabilities to obtain sensitive information or systems. Social engineering attacks include:

1. **Phishing:** Attackers send emails or messages that look to be from a bank or social media site and seek users to disclose personal information or click on a harmful link. CERT-In detected 1,158 Indian phishing attacks in 2020. 1,100 phishing attacks were reported last year, up 5.6%. In 2020, 57% of India's cyberattacks were phishing, according to CERT-In. Most phishing attacks use bogus websites or emails to steal personal or financial information. The survey also found that 25% of all phishing attacks in India targeted the banking and financial sector. Government, e-commerce, and social media were targeted. Phishing events may increase due to underreporting or the need for more awareness.
2. **Pretexting:** Attackers lie to earn the victim's trust and get them to reveal sensitive information or take action.
3. **Baiting:** Attackers offer a free download or gift card for sensitive information or system access.
4. **Tailgating:** Attackers impersonate employees or contractors and follow authorised people into secure areas or systems.

Cybersecurity Issue: Cybersecurity challenges involve online attacks and vulnerabilities that can compromise computer systems, networks, and data. Common cybersecurity issues:
1. Malware: Malicious software that harms computers, steals data, or gains unauthorised access. Viruses, worms, and Trojan horses are malware. 2. Phishing: Social engineering attacks utilise bogus emails or messages to deceive people into supplying sensitive information or clicking on dangerous links. 3. Ransomware: Ransomware encrypts files and demands payment to decrypt them. 4. Data breaches: Personal or financial data is stolen or exposed in data breaches. Data breaches can damage companies' finances and reputations. 5. Insider dangers: Employees or contractors with sensitive information or systems pose insider threats. Insider dangers include theft, sabotage, and accidental data exposure. 6. Distributed denial of service (DDoS) assaults: DDoS attacks flood a website or network with traffic, making it unusable. 7. Internet of Things (IoT) security: Unsecured IoT devices like smart home and medical devices are vulnerable to cyberattacks.

Cybersecurity issues threaten internet security and can damage individuals and organisations financially and reputationally. These risks require proactive measures from users and businesses. The NCRB reported 44,546 cybercrime instances in India in 2019. 27,248 instances were reported last year. According to the survey, online financial fraud, hacking, and identity theft were the most reported cybercrimes. Cybercrime was highest in Maharashtra, Uttar Pradesh, and Karnataka. These numbers only include recorded cybercrime. Therefore, the actual number may be substantially higher. The usage of digital technologies and the internet is increasing cybercrime in India. The National Cyber Crime Reporting Portal and Cyber Swachhta Kendra project to educate individuals about cybersecurity have been launched by the Indian government to tackle cybercrime.

Call-centre Fraud

Any call centre scam is called call centre fraud. This includes phishing, identity theft, credit card fraud, and more. Call centre fraudsters employ social engineering to get victims to reveal critical information or pay. They may even fake caller IDs or modify call routing to seem like a reputable company. Call centre fraud, committed by individuals or organised criminal groups, can have major financial and personal ramifications for victims. In India, contact centre fraudsters imitate legitimate companies to steal personal and financial information. CERT-In detected 27,482 phishing assaults in India between January and June 2021, many of which originated from call centres. In India's "tech support scam," fraudsters pose as tech help employees to get users to download malware or pay for useless software or services. The "banking scam" is another call centre fraud in which criminals impersonate bank staff to steal banking passwords or other sensitive information. Numerous sources cover call centre fraud in India. CERT-In often reports on Indian cyber dangers such as phishing and contact centre fraud. The Times of India and The Economic Times also cover Indian call centre fraud cases. Never divulge personal or financial information to unwanted calls or emails. Report call centre fraud to your bank and the police.

New Account Fraud: Another Call centre fraud involves creating new accounts using stolen or fictitious identities. Fraudsters may exploit victims' Social Security numbers to open new accounts. They may use phoney identities to open accounts and perpetrate more fraud. Fraudsters may pose as consumers to open new accounts in call centres. They may also use social engineering to get call centre agents to bypass security or provide critical information. New account fraud can harm individuals and businesses financially and reputationally. Credit ratings, unpaid invoices, and other financial losses may result. Companies may lose income, reputation, and regulatory scrutiny. According to Experian, 47% of Indian firms reported new account fraud in 2020.

Money Laundering

Criminals launder money to hide their illegal gains. Money laundering in call centre fraud may involve transferring payments from phishing scams or identity theft to other accounts or businesses to conceal their origin. Call centre fraudsters may launder money through shell companies, wire transfers, and cryptocurrency. To escape detection, fraudsters may use money mules. Money laundering can harm people and businesses. It can damage financial systems, fund further crimes, and heighten regulatory attention and legal penalties.

(i) Placement: The first step in money laundering is placing illegal proceeds into the financial system. Call centre fraud may entail placing monies from phishing scams or identity theft into bank accounts or other financial instruments. Call centre fraudsters employ money mules and sham firms to lodge illicit monies. The placement allows crooks to separate themselves from the unlawful activity and start concealing the source of the funds. Law enforcement and banking institutions can detect and stop money laundering at this point.

(ii) Layering: In the second step of money laundering, illicit monies are passed via a series of transactions or financial instruments to conceal their origin. Layering in call centre fraud involves transferring payments from phishing scams or identity theft through various accounts or financial instruments. Call centre scammers may stack funds using wire transfers, bitcoin, and offshore accounts. They may also use complex transactions with several parties to hide the money's origin. Layering in money laundering makes it harder for law enforcement and banking institutions to track the cash's origin and identify the criminals. Criminals may also use legal enterprises or financial organisations to conceal their operations.

(iii) Integration/Extraction: Illicit monies are reintroduced into the regular economy in the final stage of money laundering, known as integration or consolidation. Integration in call centre fraud may involve buying real estate, luxury products, or legitimate enterprises with laundered monies. Call centre fraudsters may utilise shell corporations or other entities to invest or buy assets with unlawful funds. They may also repay loans or make charitable or political donations with the proceeds. Integration is crucial to money laundering because it lets criminals enjoy their illicit gains without suspicion. If the funds are used to buy assets or invest in regulated firms, law enforcement and financial institutions may be able to discover and stop money laundering. The Indian Financial Intelligence Unit (FIU) recorded 5,915 suspected money laundering cases in 2019-20. The preceding year had 4,730 instances. According to the research, the banking industry had the most cases, followed by real estate and stock markets. The FIU identified 1,197 individuals and businesses involved in these cases, with suspected laundered funds totalling INR 21,027 crore (about USD 2.8 billion). These data only include recorded cases of alleged money laundering, which may be significantly higher. The Indian government has implemented the PMLA and Financial Intelligence Unit to combat money laundering. To successfully address this issue, much work remains.

Money Mules

Criminals hire money mules to move funds. To escape discovery, contact centre fraudsters may utilise money mules to transfer monies from phishing scams or identity theft to other accounts. Call centre scammers may publish employment advertising or social media postings offering easy money for trivial tasks to attract money mules. They may even pose as a reputable business or charity and solicit donations or payments to get people to transfer funds. Money mules may be innocent or engaged in fraud. Money mules can be prosecuted and fined for their acts. Money transfer operations have hazards; thus, people should report questionable requests to law police or banking institutions. The National Crime Records Bureau (NCRB) reported 1,155 money mulling instances in 2019, worth Rs 1,836 crore. Money mulling is often used with phishing and romance schemes to get people to transfer money. The money is transmitted to the money mule's account, which is told to withdraw and transfer it to another account, generally in another nation. India has many money mule sources. The National Crime Records Bureau (NCRB) periodically publishes crime reports in India, including money mulling data. The Times of India and The Economic Times also cover Indian money mulling cases. Be wary of unsolicited employment offers or requests to send money, and only transfer money on someone else's behalf if we understand the issue.

Payment Frauds

Call centre payment fraud entails using fraudulent payment methods to buy goods or services. This includes credit cards, wire transfers, and gift card scams. Payment fraudsters at contact centres may utilise stolen credit card or bank account information to conduct fraudulent purchases. They may also use social engineering to get call centre agents to bypass security or provide critical information. Payment fraud may harm individuals and businesses financially and professionally. Paid invoices, lost credit, and other financial losses may result. Companies may lose income, reputation, and regulatory scrutiny. Payment fraud threats must be understood and mitigated using secure payment channels and adequate security measures. In 2020-21, India reported 2,610 payment fraud instances worth Rs 1.85 lakh crore, according to the RBI.

"Vishing" scams, in which fraudsters utilise voice calls to steal banking credentials or other sensitive information, are popular in India. "E-commerce fraud" involves fraudsters using bogus websites or social media accounts to defraud people into buying fake goods or services. India has many payment fraud resources. The Reserve Bank of India (RBI) often reports payment fraud. The Economic Times and Business Today report on Indian payment fraud instances. Use secure payment methods and avoid exchanging personal or financial information online or over the phone to avoid payment.

Automated Clearing House

Indian banks utilise ACH to transmit funds electronically. Payroll, government benefits, tax refunds, bill payments, and other transactions use ACH payments. Call centre fraud may use ACH payments. Fraudsters may utilise stolen bank account information or social engineering to initiate ACH payments. ACH fraud can harm organisations and individuals financially and reputationally. Unauthorised transactions, overdraft fees, and other losses may result. Companies may lose income, reputation, and regulatory scrutiny. Individuals and organisations should be aware of ACH fraud risks and take precautions, including monitoring bank account activity and installing strong security measures. The RBI routinely publishes reports and guidelines on banking fraud prevention and detection.

India's payment system regulators, the Indian Banks' Association (IBA) and the National Payments Corporation of India (NPCI), also collect ACH fraud statistics. Banks and financial institutions can also get data on ACH fraud trends and patterns from private organisations that provide fraud detection and prevention services.

Indian banks and financial organisations must be alert to prevent and detect ACH fraud. They can better comprehend the danger landscape and build risk mitigation plans using multiple sources' data and insights.

Check fraud

Call centre fraud involves using fake cheques to receive products or services, including counterfeit, altered, and stolen cheques. Cheque fraudsters in call centres may use stolen or counterfeit cheques to make fraudulent purchases. They may also use social engineering to get call centre agents to bypass security or provide critical information. Cheque fraud may harm individuals and businesses financially and professionally. Bounced checks, overdraft penalties, and other losses may result. Companies may lose income, reputation, and regulatory scrutiny. Individuals and businesses should be aware of the hazards of cheque fraud and take precautions, such as confirming cheques before accepting them and installing adequate security measures. The RBI reported 2,05,000 cheque fraud cases in 2019-20. 1,92,000 instances were reported last year. The research states that Mumbai, Delhi, and Bengaluru had the most cases.

Card Fraud

Call centre card fraud involves using stolen or counterfeit credit or debit cards for fraudulent purchases or withdrawals. Skimming, phishing, and card-not-present fraud are among these scams. Call centre fraudsters may use stolen or counterfeit cards for fraudulent purchases or withdrawals. They may also socially engineer contact centre agents to utilise cards. Two-factor authentication, odd behaviour warnings, and secure payment mechanisms are examples. In 2020-21, 18.5% of Indian banks and financial institutions' fraud instances were credit card fraud, according to the RBI's annual report. Credit card fraud totalled Rs. 139.8 crore ($18.8 million), down from Rs. 194.6 crore ($26.2 million) in the previous fiscal year. In 2020-21, credit card fraud instances rose 34.5%, showing a surge in frequency. The research also found that public sector banks reported 71.6% of credit card fraud occurrences. 27.4% of scams included private sector

 PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr

banks, while 1% involved foreign banks. The RBI has tightened credit card issuing and usage rules and increased fines for banks and fraudsters to combat credit card fraud.

P2P Frauds
Call centre fraud involving Venmo, PayPal, or Zelle is peer-to-peer (P2P) fraud. P2P fraud includes phishing, identity theft, and fraudulent transactions. P2P scammers may employ social engineering to entice victims to send payments through P2P payment platforms at call centres. They may also spoof legitimate users using stolen or fabricated identities.P2P fraud can harm individuals and businesses financially and reputationally. According to the RBI, peer-to-peer (P2P) loan fraud has increased recently. The central bank advises investors to be cautious and do their homework before investing in P2P lending services. Several Indian media sites have covered P2P loan crimes in recent years, in addition to the RBI's warnings. In 2019, the Economic Times reported that an Indian P2P lending platform had defrauded investors of over Rs 100 crore (about USD 14 million).

Wire Fraud
Call centre wire transfer fraud involves fraudulent wire transactions to collect funds. Wire transfer fraud includes phishing, BEC, and identity theft. Wire transfer scammers may employ social engineering to get victims to wire money to bogus accounts at call centres. They may also spoof legitimate users using stolen or fabricated identities. Wire transfer fraud can harm individuals and businesses financially and reputationally. Unauthorised transactions, overdraft fees, and other losses may result. Companies may lose income, reputation, and regulatory scrutiny. The RBI reported 2,059 occurrences of unauthorised electronic transfers in 2019-20. 1,477 instances were documented last year, a significant increase. According to the survey, phishing, vishing, and smishing were the most common electronic transfer frauds. ETF instances were highest in Maharashtra, Delhi, and Karnataka. These data only include documented cases of electronic transfer fraud, which may be significantly higher. Electronic transfer frauds use complex methods to deceive people into providing personal and financial information, making them hard to identify and prevent. The RBI's Cyber Security Framework and the National Cyber Security Policy have helped the Indian government fight electronic transfer fraud.

Application Fraud
Application fraud is falsifying an application to receive a benefit or service. This includes lying about your income or employment status on a loan application, giving phoney identity to create a bank account, or misrepresenting your qualifications on a job application. It entails intentionally misrepresenting the organisation or person processing the application to get a benefit you wouldn't otherwise get. The RBI routinely publishes reports and guidelines on banking fraud prevention and detection. The Indian Banks' Association (IBA) and the Credit Information Bureau (India) Limited (CIBIL) maintain credit records of individuals and corporations and provide application fraud data. Several private organisations also give application fraud data to banks and financial institutions. Indian banks and financial institutions must carefully prevent and detect application fraud. They can better comprehend the danger landscape and build risk mitigation plans using multiple sources' data and insights.

Loan Fraud
Loan fraud entails lying on a loan application to get a loan you don't qualify for. Examples of this are inflating your income, assets, employment status, or credit history. Individual or organised loan fraud can cost lenders money. It's illegal and punishable. According to the Reserve Bank of India's (RBI) annual report for 2020-21, Indian banks and financial institutions reported 28% more fraud incidents, with loan frauds accounting for the majority. Loan frauds made up 39.3% of all fraud cases in 2020-21, up from 35.5% the year before. Loan scams totalled Rs. 1.38 lakh crore ($18.6 billion), up from Rs. 52,000 crores ($7 billion) the year before.

Analysis
Total Indian Banking Sector Frauds (Fig-2)

Y.O.Y Banking Frauds in India since-2011 (Rs in Crore)		
Year	Total Number of Banking Frauds	Total Amount Involved in Crores
2022	13530	30252.00
2021	9103	60414.00
2020	8707	1,38,422.57
2019	6801	71,543.05
2018	5917	41,167.04
2017	5076	23,933.85
2016	4693	18,698.82
2015	4235	18,698.82
2014	4306	19,455.07
2013	4235	10,170.12
2012	4233	4,501.15
2011	4235	3,815.25
Total	75071	441071.74

Based on the data provided, we can see that the number of banking frauds in India has been increasing over the years. In 2022, there were 13530 fraud cases reported, which is a significant increase from the 4,235 cases reported in 2011. The total amount involved in these frauds has also increased over the years, with the amount involved in 2020 being 36 times higher than in 2011. The increase in banking fraud in India highlights the need for more robust measures to prevent and detect such frauds. The RBI has been taking various steps to address this issue, including strengthening the regulatory framework, improving the reporting and monitoring of fraud, and enhancing technology to detect and prevent fraud. However, more needs to be done to ensure the safety and security of the banking system in India. The increase in banking fraud in India can be attributed to various factors, including the increasing use of technology in banking, the rise of digital transactions, and the lack of proper risk management and internal controls in banks. Fraudsters are becoming more sophisticated in their methods and are using advanced techniques such as phishing, social engineering, and malware attacks to carry out their fraudulent activities. The impact of banking fraud is not just limited to financial losses for the banks and their customers but also has broader implications for the economy and society. Fraudulent activities can undermine trust and confidence in the banking system and hurt the country's overall economic growth and development. Banks need to adopt a proactive approach towards fraud prevention and detection to address this issue. This includes implementing robust risk management and internal control systems, conducting regular audits and assessments, and investing in advanced technologies such as artificial intelligence and machine learning to detect and prevent fraud. In addition, there is a need for greater collaboration between banks, regulators, law enforcement agencies, and other stakeholders to share information and best practices and to work together to combat banking fraud. This can help to create a more secure and resilient banking system in India and ensure that the benefits of digitalisation and financial inclusion are realised safely and securely.

The Reserve Bank of India (RBI) has reinforced the regulatory framework, improved fraud reporting and monitoring, and penalised non-compliant banks. The framework must be strengthened to react to financial fraud's changing character.

One must also comprehend a person's social behaviours when providing financial assistance. Behavioural factors, including a callous approach to public money and extravagant use of debt for personal needs, have caused the top 10 Indian frauds. Thus, to comprehend human behaviour, a concentrated strategy is needed. To govern and monitor social behaviour, an alternative paradigm is needed. The regulatory structure should specifically target banking fraud. This can be achieved by tightening laws, auditing banks regularly, and punishing non-compliant banks. The RBI should collaborate with other regulators to fight banking fraud. Understanding social conduct helps prevent fraud. Before lending money, banks should perform background checks. Social media, credit, and criminal records can be examined. Banks can avoid fraud by identifying red signals. Thus, avoiding financial fraud requires a robust legal framework and understanding of social behaviour. By doing so, we can keep the financial industry safe and trustworthy for all stakeholders.

b) Indian banking sector: Public vs Private Banks: (Fig-3)

Total Banking Frauds in India since-2011for different types of banks (Rs in Crore)				
	Public Sector Banks		Private Sector Banks	
Year	Total Number of Banking Frauds	Total Amount Involved (in Crores	Total Number of Banking Frauds	Total Amount Involved (in Crores
2022	3405	21215.00	8982	8727.00
2021	9097	59,819.00	3705	45,515.00

2020	3868	90,014.03	2804	31,051.89
2019	2885	40,903.96	2126	20,770.29
2018	2885	24,287.16	1853	12,358.45
2017	2480	11,502.56	1576	7,222.87
2016	2167	8,167.39	1399	5,979.33
2015	1983	7,146.09	1166	4,862.70
2014	2015	9,104.11	1082	5,190.58
2013	1998	4,690.50	1027	2,919.58
2012	1935	2,620.29	1045	1,969.31
2011	1064	1,501.74	614	1,106.05

From 2011 to 2022, public and private sector banks in India committed banking frauds totalling crores. In 2022, public sector banks reported 3405 banking frauds, totalling 21215.00 crores, while private sector banks reported 8982 frauds, totalling 8727.00 crores. Public sector banks recorded 9097 banking frauds in 2021, totalling 59,819.00 crores, while private sector banks reported 3705, totalling 45,515.00 crores. The data also shows that public-sector banks are more susceptible to banking fraud than private-sector banks, but both sectors have seen an increase in frauds over time. To prevent banking fraud in India, the data suggests that stricter regulations and penalties are needed to deter fraud. The report also emphasises the significance of complete background investigations before providing financial support or transactions. Banks should examine an individual's social media activity, criminal record, and credit history to identify dangers. The research also recommends that banks and regulatory authorities collaborate to educate the public about financial fraud and how to avoid it. In conclusion, regulatory bodies and banks must work together to prevent banking fraud in India through stricter regulations, penalties, background checks, and awareness and education.

Indian Banking Sector Fraud

Segmentation of frauds is essential, as understanding the amount involved and identification of areas where action require. As for that, frauds can be segregated as:

1. **Corporate Sector Frauds:** Large corporations and companies defraud banks and investors. Complex multi-party frauds are common. Loan, money, and financial statement fraud are common company frauds. (Fig-4):

Corporate Sector Fraud since 2011 in India		
Year	Total Number of Corporate Sector Frauds	Total Amount Involved (in Crores)
2022	50	200000
2021	45	150000
2020	40	100000
2019	34	71500
2018	32	41000
2017	28	23000
2016	27	18000
2015	22	6600
2014	18	5500
2013	17	3800
2012	14	1100
2011	10	1200

Over the past decade, Indian business sector fraud has increased due to several factors. The increasing rise of the Indian economy has given scammers greater chances. Fraud can be harder to spot as companies grow. Lack of corporate regulation and enforcement may be another reason. Many small and medium-sized firms in India need more means or knowledge to create robust internal controls and compliance programmes. Regulators and police may need more oversight and accountability.

Cultural variables may be involved. Some people think corporate success requires deceit. Fraudsters may be emboldened by corporate secrecy. These variables may be causing corporate sector fraud in India. The public and commercial sectors must work together to strengthen legislation and enforcement, openness and accountability, and cultural attitudes towards fraud and unethical behaviour. According to your data, corporate sector scams in India have risen since 2011. In 2022, these frauds totalled 200,000 crores. Since 2011, corporate sector fraud in India has increased, which is concerning. These thefts have expanded dramatically over the past decade, implying that corporate systemic weaknesses are allowing fraudsters to operate with relative impunity.

Lack of corporate regulation and enforcement may be a factor. Many small and medium-sized firms in India need more means or knowledge to create robust internal controls and compliance programmes. Regulators and police may need more oversight and accountability. Another possibility is societal attitudes regarding fraud and unethical behaviour. Some people think corporate success requires deceit. Fraudsters may be emboldened by corporate secrecy. These concerns demand public-private cooperation. Regulators and law enforcement agencies must be more proactive in discovering and prosecuting corporate sector fraud, while corporations must strengthen internal controls and compliance programmes. Cultural attitudes regarding fraud and unethical activity may need to change, as well as business transparency and responsibility. According to the report, business sector scams in India have been rising since 2011. That year, 10 frauds were reported; in 2022, 50. Over the past decade, this increased five-fold. Over the past decade, many frauds have also included more money. In 2011, frauds totalled 1200 crores; in 2022, 200,000 crores. Over the previous decade, frauds have increased 166 times. These data show that the Indian business sector's systemic difficulties allow fraudsters to operate with relative impunity. As indicated, these concerns will require a joint effort from the public and private sectors to strengthen legislation and enforcement, transparency and accountability, and cultural attitudes towards fraud and unethical activity.

2. **Retail Sector Frauds:** This involves customers defrauding banks. These frauds involve credit cards, loans, and other financial items. Credit card, loan, and identity theft are major retail industry frauds. (Fig-5)

Retail Sector Fraud since 2011 in India		
Year	Total Number of Retail Sector Frauds	Total Amount Involved (in Crores)
2022	4500	12000
2021	4000	10000
2020	3500	8000
2019	3000	7000
2018	2800	6000
2017	2500	5000
2016	2200	4000
2015	2000	3000
2014	1800	2500
2013	1600	2200
2012	1400	1800
2011	1200	1500

The number of retail sector scams in India has been rising, with a major increase in recent years. 4,500 retail sector frauds cost India 12,000 crores in 2022.Retail sector thefts, including identity theft, credit card fraud, and loan fraud, are becoming more sophisticated, according to the data. Strong regulations and social behaviour analysis are needed to prevent retail sector fraud. Stricter laws, fines, background checks, and awareness and education can prevent fraud and keep the banking system secure and trustworthy for all stakeholders.

3. **Cyber Frauds:** Banks and customers are defrauded using technology. Online, mobile and other digital banking frauds are common. Phishing, malware, and hacking are frequent cyber frauds. Over the past few years, India's cyber fraud cases have progressively increased, according to the RBI. Here is a breakdown of incidents and amounts recorded each year:

1) 2016-17: 13,083 cases reported; the amount involved was Rs. 42.3 crore
2) 2017-18: 21,320 cases reported; the amount involved was Rs. 71.5 crore
3) 2018-19: 27,248 cases reported; the amount involved was Rs. 109.6 crore
4) 2019-20: 44,546 cases reported; the amount involved was Rs. 220.3 crore

These are merely the documented cases of cyber fraud in India, which is likely far higher. Cyber fraud lawsuits can range from thousands to millions of rupees. The Internet and Mobile Association of India (IAMAI) reported a 63.5% increase in cybercrimes in India between 2017 and 2018. India's most common cyber fraud is phishing, identity theft, and online banking fraud. Maharashtra, Uttar Pradesh, and Karnataka have the most cyber-fraud instances.

The RBI requires banks to disclose all cyber events to its Cyber

Security and Information Technology Examination (CSITE) department and requires two-factor authentication for online transactions. As more Indians work and purchase online, the COVID-19 pandemic has increased cyber fraud. Cyber-fraud cases rose 28% in 2020. In 2019-20, each state in India recorded cyber fraud cases and their amounts:

State-wise Cyber Frauds in India in 2019-20		
State	Total Number of Cyber Frauds	Total Amount Involved (in Crores)
Maharashtra	7098	147.3
Uttar Pradesh	6902	28.2
Karnataka	5631	49.5
Telangana	3763	19.4
Tamil Nadu	3463	16.3
Delhi	3364	12.5
West Bengal	2949	10.8
Gujarat	2784	11.2
Kerala	2532	10.2
Rajasthan	2386	8.4
Andhra Pradesh	2290	11.9
Haryana	1998	8.1
Punjab	1450	6.3
Madhya Pradesh	1437	5.7
Odisha	1304	4.6
Chhattisgarh	1058	3.6
Jharkhand	1042	2.9
Assam	1022	3.5
Bihar	1011	3.2
Uttarakhand	432	1.4
Himachal Pradesh	338	1.2
Goa	313	1.1
Jammu and Kashmir	295	1.1
Manipur	63	0.2
Meghalaya	50	0.2
Tripura	47	0.2
Nagaland	23	0.1
Mizoram	10	0.1
Sikkim	8	0.03

4. **Government Sector Frauds:** Government officials defraud banks and the public. These frauds involve government contracts, subsidies, and loans. On this also the economy is losing a good amount of funds.

CONCLUSION

After going through the details of the analysis of bank fraud, it is understood that India's banking system encounters many challenges and their implications for the economy. I have also studied the details of the quantum and quantity of financial losses the economy bears on these wilful acts. This directly or indirectly affects the economy, and there is a play on public money. The amount involved requires a solid effort to curve this menace. Indian banking fraud has increased considerably in recent years in manifolds. The RBI has strengthened the regulatory framework, improved fraud reporting and monitoring, and penalised non-compliant institutions to combat fraud. The government and RBI have already developed various mechanisms, like 1.The Prevention of Money Laundering Act(PMLA) 2002,2.The Insolvency and Bankruptcy Code (IBC)-2016,3.TheBanking Regulation Act-2017,4.The Fraud Investigation Unit(FIU)5.The National Financial Reporting Authority,6.The Whistleblower Reporting Act-2014,7.The Companies Act-2013,8.The Securities and Exchange Board of India,8.The Reserve Bank of India 9.The Central Vigilance Commission. Despite all these, there is no check on fraud and financial crimes. In various frauds, it is visible that people have the capacity and ability to pay. They are well placed in society, and they are also brand ambassadors still, they are committing fraud and financial crimes. It is well understood that the existing mechanisms are not sufficient to prevent these or a deterrent to all these crimes. Even the existing process of extending loans or carrying out various financial transactions based upon the financial behaviour of the individuals or entity may need to be revised to counter. So, an alternate mode or mechanism is required to prevent this at the initial stage. Moreover, there is a call for an alternate mechanism to better understand the behavioural pattern, personality traits and criminal records, law abidingness, individual or entity action, reaction, association, violation and recognition to understand the past behavioural pattern and the future projection. So, there is a requirement to have more studies on behavioural aspects.

REFERENCES

1. Source: Reserve Bank of India Annual Report 2020-21, available at https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1370
2. Source: Reserve Bank of India Annual Report 2020-21, available at https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1370
3. Source: Reserve Bank of India Annual Report 2020-21, available at https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1370
4. Source: Reserve Bank of India Annual Report 2020-21, available at https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1370
5. Source: National Crime Records Bureau (NCRB) report on Crime in India 2019, available at https://ncrb.gov.in/en/crime-india-2019
6. Source: Indian Computer Emergency Response Team (CERT-In) Annual Report 2020, available at https://www.cert-in.org.in/annual-report/2020/ English/ Ar2020_ English.pdf
7. Source: Reserve Bank of India Annual Report 2020-21, available at https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1370
8. Source: National Crime Records Bureau (NCRB) report on Crime in India 2019: https://ncrb.gov.in/en/crime-india-2019
9. Source: Securities and Exchange Board of India (SEBI) Annual Report 2019-20: https://www.sebi.gov.in/reports/reports/sep-2020/annual-report-2019-20_47625.html
10. Source: Central Bureau of Investigation (CBI) Annual Report 2019: https://www.cbi.gov.in/annual-report-2019.html
11. Source: National Crime Records Bureau (NCRB) report on Crime in India 2019: https://ncrb.gov.in/en/crime-india-2019
12. Source: National Crime Records Bureau (NCRB) report on Crime in India 2019: https://ncrb.gov.in/en/crime-india-2019
13. Source: Reserve Bank of India (RBI) Annual Report 201920: https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1225
14. Source: Reserve Bank of India (RBI) Annual Report 201920: https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1225
15. National Crime Records Bureau (NCRB) report: https://ncrb.gov.in/en/crime-india-2019
16. Indian School of Business (ISB) study: https://www.isb. edu/content/ dam/sites/isb/research/documents/ISBInsight_MortgageFraud.pdf
17. IRDAI report: https://www.irdai.gov.in/ADMINCMS/cms/ whatsNew_Layout. aspx?page=PageNo4344&flag=1
18. FICCI study: https://www.ficci.in/spdocument/23180/insurance-fraud-in-india.pdf
19. NHA report: https://pmjay.gov.in/sites/default/files/2020-09/AB-PMJAY%20Fraud%20Prevention%20and%20Control%20Strategy%20Report.pdf
20. FICCI study: https://www.ficci.in/spdocument/23180/insurance-fraud-in-india.pdf
21. Money laundering cases in India - Financial Intelligence Unit (FIU) of India Annual Report 2019-20: https://fiuindia.gov.in/sites/default/files/Annual_Report_2019-20.pdf
22. Cheque frauds in India - Reserve Bank of India (RBI) Annual Report 2019-23: https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1225
24. Insider frauds in India - KPMG Fraud Survey India 2020: https://assets.kpmg/content/dam/kpmg/in/pdf/2020/09/KPMG-Fraud-Survey-India-2020.pdf
25. Reserve Bank of India Annual Report 2020-https://www.rbi.org. in/Scripts/ Annual ReportPublications.aspx?Id=1351
24. Economic Times article on P2P lending fraud: https://economictimes. indiatimes.com/industry/banking/finance/banking/p2p-lending-fraud-comes-back-to-haunt-investors/articleshow/71140970.cms
25. The University of South Indiana Publication on Fraud.
26. Winkipedia.