https://doi.org/10.58419/gbs.v11i2.1122518

AN ANALYSIS OF CYBER FRAUDS IN BANKING SECTOR A CASE STUDY OF SBI KARNATAKA DIVISION

Ms. Keerti Reddy
Research Scholar
Department of Management Studies, Visvesvaraya Technological University, Belagavi
keertireddy2328@gmail.com
Dr. Basavaraj Kudachimath
Associate Professor
Department of Management Studies, Visvesvaraya Technological University, Belagavi
bskudachimath@gmail.com

Abstract:

This study investigates how banking automation and rapid digital expansion have shaped cyber fraud in the State Bank of India's Karnataka division over the period five years. The study concentrates on two variables annual cyber fraud incidents and total money involved in such cases. A descriptive, quantitative time series design is used to determine directionality and magnitude of change in the incidence of fraud and financial loss.

The findings indicate a steep growth in the frequency and amount of cyber fraud with a substantial peak followed by a moderation. AI-powered services and digital platforms have increased efficiency and reduced friction. The paper finds that cyber fraud has been transformed into a structural risk within an automated banking environment and suggests that continued investment in cyber security controls, fraud analytics, staff skill and customer education is important to ensure the gains from digital Banking transformation are not lost to new-age threats.

Keywords

State bank of India, Cyber frauds, Banking automation, Digital banking, Trend analysis, Karnataka division.

Source of fund: The research is self-funded

Conflict of interest: There is no conflict of interest to be declared

INTRODUCTION

The State Bank of India is the largest commercial bank and financial services company in terms of assets. In the past five years (2020 - 2025). "SBI is a classic combination of an old traditional giant and technology driven upstart coming together to reinforce each other, paving the way for an exciting future that includes both past and the future", Manghnani said. Sbi One of the biggest. Yet, to cope up with a crore of customer base, banks do have competition, change in service at digital age and productivity as well as efficiency, and then second would be cyber threat.

SBI is losing customers, on the other hand. Providing the guarantee to over 520 million beneficiaries every year by 2025 would be an economic lifeline for most Indians. SBI is adding around 65,000 new users on a daily basis as a run rate of its pack. There are 23000 branches, 62,000 ATMs & a highly popular growing digital platform in YONO, which has over 90 million registered users and is present in transactions by about ten million daily active users. So that people can open a new account and apply for a loan and do transactions without ever having to go into the branch at all, much instinct convenience in today's banking world.

The rapid customer expansion is also translating into strong financial growth. SBI Q2 FY25 net profit was at Rs. 20160 crore, which was also 10% higher on a YoY basis, and profits have been steadily growing. It has also done well, as part of this effort, to clean the balance sheets and raise the quality of assets in proportion to risk. The NPA ratio decreased from 1.82% to 1.73%, and the manageability of bad loans level was relatively higher by bank. Total advances have crossed 42 Lakhs crore and deposits 52 lakh crore. SBI is a leading role player in the credit and deposit system of India.

Behind all This SBI has also adopted automation in order to keep up with these massive operational needs. Exposure to automation. The bank uses Robotic Process Automation (RPA), which automates mundane back office tasks like loan applications and compliance monitoring, to reduce both processing time and risk of errors. From smart scoring of credit through fraud detection all the way to service chat bots that customer services has even faster help on, already in self-servic and then we are also able to digitalise behaviour just as quickly. Technology is already trying itself out, we can see it with money, it's impenetrable, it's secure and transparent. This not only improves efficiency of operations for SBI but also allows it to take newer age and new-age modern channel products to market faster in India with it's retail consumers or at least light up some millions middle class to bank with SBI in India.

But the online leap is also accompanied by an increased risk of cyber-attacks. SBI had built-in social responsibility in the form of AI-driven fraud detection, hard core value-based financial limits with Two-Factor authentication as a necessity, real-time scan across transactions and sustained consumer education. These are the differences that keep customer funds and trust protected in an era of increasing cyber-threats.

OBJECTIVES

1. To identify the number of cyber frauds in SBI
2. To identify the reasons for cyber frauds

THEORETICAL BACKGROUND

Financial intermediation

Banks like SBI are pivotal in linking the savers and lenders of the economy by mobilising deposits for lending purposes. SBI is capable of enabling financial mirage and spawning economic activity mainly in the banks it lends to. And that core conviction is one of the two reasons SBI has doubled in size over the past five years.

Diffusion of innovation

Banking remains on the new tools and techniques path, but technology is two steps ahead. The apparent digitisation which SBI has kick-started with mobile apps, digitised process etc are evidence that till now all of us have seen only innovation in day-to-day banking. And with these services becoming increasingly commoditised, so too has contact with the customer in the branch.

Resource - based view

The banks also need to conserve and extend their valuable resources for further development of the society. SBI's good customer service and focus on solid infrastructure and security have enabled it to quickly react to changes in the market. This emphasis on developing the strengths has transformed the bank into a strong and competitive organisation.

Risk management

As banking services increasingly go online, contemporary banks are now subject to additional risks. With SBI’s expansion, the flipside is that we have to be more prescriptive in our affiliation to counter risks from credit defaults to cyber risk. The bank and its millions of customers are protected by having a robust security and fraud prevention system in place.“

LITERATURE REVIEW

Growth of State Bank of India

Empirical studies on SBI’s post Covid period show that digital initiatives such as the YONO platform, mobile and internet banking have contributed to a steady expansion of the bank’s asset and deposit base and to improved profitability indicators. Analyses of SBI’s financial performance conclude that the bank maintained healthy liquidity and solvency positions between 2020 and 2025, despite macroeconomic uncertainty, by leveraging technology to widen its customer base and deepen penetration in semi urban and rural markets (kumar, 2024). Several papers emphasize that SBI’s integrated digital super app model and its focus on end to end analytics have enhanced cross selling opportunities and operational efficiency while supporting financial inclusion objectives. These studies also note that rising digital transaction volumes through YONO and other platforms have reshaped customer behavior, increasing reliance on remote channels and reinforcing SBI’s competitive position in the Indian banking system (Mehta, 2024)

Prevalence and threats of cyber fraud in SBI and Indian banks

Research on cyber risk in Indian banking documents that a majority of reported frauds now involve technology based channels such as internet banking, cards and mobile payments, with one widely cited study finding that around 65% of fraud cases are linked to technology related channels. Journal articles using Reserve Bank of India data show that the number and value of digital fraud incidents have risen sharply in recent years, with online payment fraud, card not present transactions and unauthorized electronic transfers emerging as dominant modes (M, 2024).Studies in applied finance and management journals identify hacking, phishing, malware based intrusions and social engineering attacks as the main external vectors of fraud, often exploiting customer inexperience and weak verification on digital interfaces. At the same time, research on operational risk stresses that insider collusion and internal control lapses remain significant, particularly in large public sector banks, amplifying the threat landscape beyond purely external cyber-attacks (bindhushree, 2024). Recent industry oriented and academic analyses acknowledge that SBI and peer banks have strengthened their fraud risk frameworks through real time monitoring systems, anomaly detection and customer awareness campaigns these studies argue that the sheer growth in digital transaction volumes, coupled with increasingly sophisticated attack methods, has led to an overall increase in the absolute number of fraud cases and in aggregate financial losses, even where detection capabilities have improved (barik, 2025)

Reasons for cyber frauds in banking sector

Research across Indian and international journals converge on several structural drivers of rising cyber fraud in banks such as SBI. High transaction volumes on digital channels, accelerated by post pandemic behavioral shifts, expand the attack surface and create more opportunities for exploitation of system and process vulnerabilities. Studies in technology and management journals further highlight the growing sophistication of cybercriminals, who routinely employ advanced phishing kits, malware, credential stealing tools and social engineering scripts tailored to banking customers (kumar A. , 2022). Insider enabled fraud emerges as a distinct concern in the literature, with papers on Indian bank frauds documenting cases where employees misuse access rights, override controls or collude with external actors to facilitate unauthorized withdrawals and data leakage. These studies consistently argue that robust internal controls, segregation of duties, regular system audits and rigorous background screening are essential for mitigating such risks in large institutions (roy, 2024).

METHODOLOGY

This study uses quantitative data for evaluating the changing phase of SBI since 2020 to 2025. This study includes

1. Number of cyber fraud cases registered in SBI each year during last five year (2020-2025)
2. The total amount involved in these cyber frauds in five years(2020-2025)

RESEARCH DESIGN

- The study uses quantitative, descriptive time series research design focusing on secondary data for five consecutive years.
- The design aims to identify and explain the directional changes (upward or downward trend) in the number of cyber fraud cases and the amount involved

Data collection and study period

The analysis is based on the secondary data, given by SBI through Right to Information Act - 2005, where SBI has given information regarding

- Number of cyber frauds cases registered in SBI each year during last five years (2020-2025)
- The total amount involved in these cyber frauds in last five years(2020-2025)

Variables

- Time variable: financial year coded as an time Index t =1, 2,3,4,5 for 2021-22 to 2024 -25. This is the independent variable in the trend regression.

- Outcome variable: 1. number of cyber fraud cases in SBI each year and 2. Total amount involved in these cyber frauds each year (in lakh) both treated as time series dependent variables.

DATA ANALYSIS TECHNIQUES:

The method of study was a Quantitative Time series research and secondary data were used for 5 years beginning from 2021-22 to 2024-25.

Descriptive statistics- descriptive data was first used to summarise the annual rates of cyber frauds and the amount, in totality, mean or percentage changes over time and presented using tables, line/column for ease of visuals to show year-on-year fluctuations.

Both models were tested against the time trend model using a trend analysis. To estimate the trend and type of change that they represent, a simple linear regression model, Y = a+bx was fitted separately to the number of cyber fraud cases as well as the amount involved, with x being the coded year index. According to the coefficient estimated, trend value per year was computed as well as interpreted on average annual rise of cases and financial loss during the period of study.

Analysis software: Data were collected, organized and analysed in Microsoft Excel and trend values and descriptive statistics were calculated using this facility. Trend over time was calculated and plotted using line chart and trend line tools in Microsoft Excel. Microsoft Excel was used for preliminary data cleaning, time-trend value determination, and to plot the time series graph.

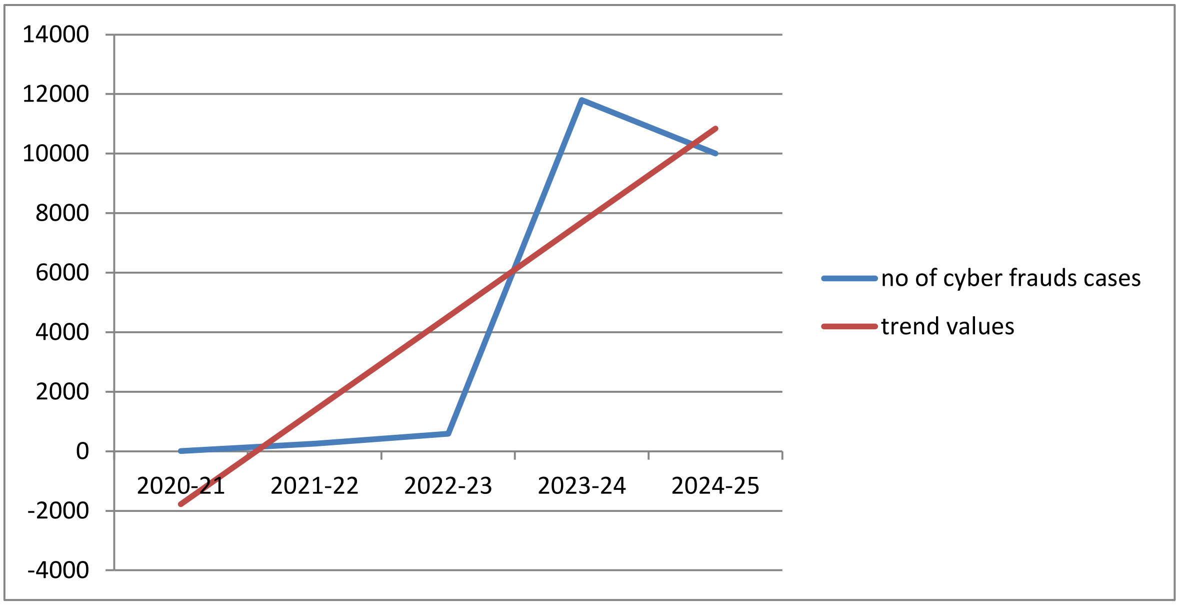
DATA ANALYSIS AND INTERPRETATION

Table 1: descriptive statistics

Trend values for the number of cyber fraud cases in SBI Karnataka division since 2020-21 to 2024-25

SI NO	Year	Number of cyber fraud cases	Trend values
1	2020-21	4	-1777.6
2	2021-22	259	1376.8
3	2022-23	587	4531.2
4	2023-24	11801	7685.6
5	2024-25	10005	10840

Diagram 1: Trend analysis of number of cyber frauds in SBI karnataka division since 2020-21 t 2024-25



Interpretation

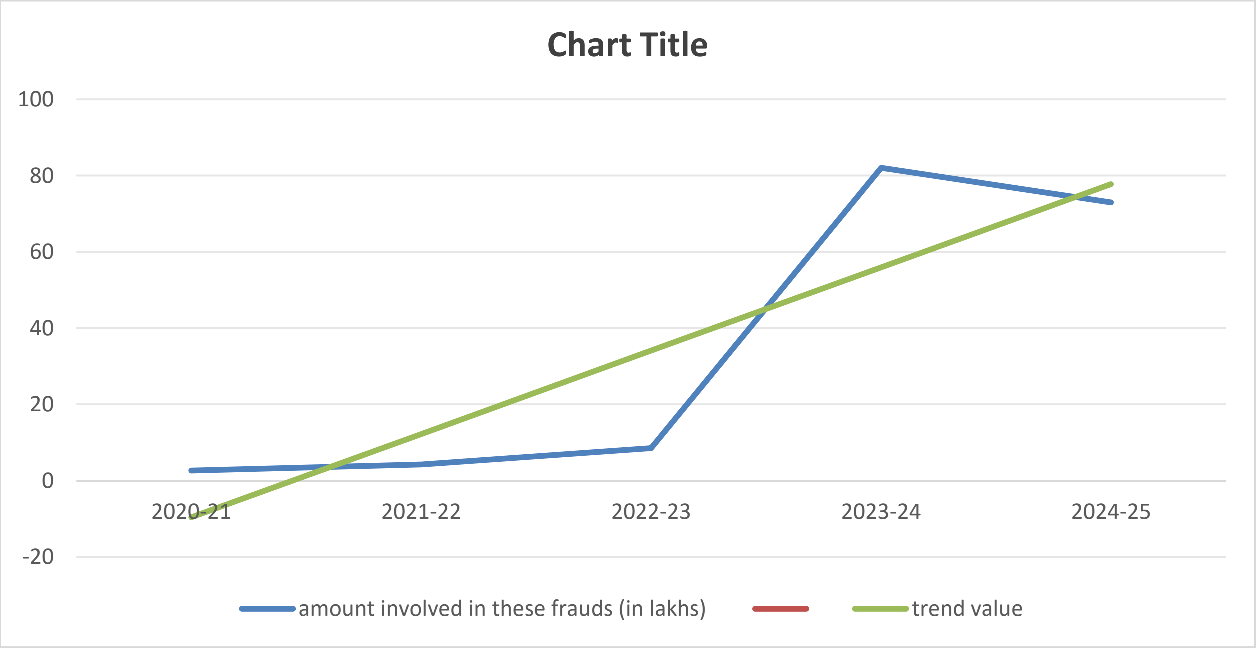
The number of cyber frauds in SBI is increasing every year. It was just 4 in 2021 and reached to 10005 in 2024-25. The trend value shows an increase in number of cyber frauds. The diagram shows that the frauds in 2022-23 are far below the average frauds, and in 2023-24, it is far above the average trend. It's another way of saying that the deviation in the number of cyber frauds number is too much every year.

It could in fact, go even higher, based on the average prediction of the frauds in future years. The bank has taken meticulous detection process to check such frauds for banking sector of SBI. Therefore, the frauds have diminished. There is a fraud reduction of about 15.3%, but still the frauding cases are going on a large scale. Hence bank is bound to stop the fraud.

Table 2: Trend values for the amount involved(in lakhs) in these cyber fraud cases in SBI Karnataka division since 2020-21 to 2024-25

SI NO	Year	Amount involved in the cyber frauds (in lakhs)	Trend value
1	2020-21	2.64	-9.61
2	2021-22	4.23	12.244
3	2022-23	8.57	34.098
4	2023-24	82.05	55.952
5	2024-25	73	77.806

Diagram 2: Trend analysis for the amount involved in these cyber frauds cases in SBI Karnataka region since 2020-21 to 2024-25



Interpretation : The table and the analysis represents both the amount involved in the cyber frauds and the fitted trend values generated from linear regression model for the period 2020-21 to 2024-25. The regression line shows a steadily rising trend with the trend value increasing from -9.61 lakh in 2020-21 to about 77.81 lakh in 2024-25 indicating a strong upward trajectory in the expected financial impact of cyber frauds over a time.

In first three years the actual amount (2.64, 4.23 and 8.57) remain relatively closer to below the corresponding trend values, shows that losses were still in an early growing phase and broadly consistent with the underlying upward pattern shown by the model. From 2023-24 onwards the gap between the actual and trend values become substantial. In 2023-24 the actual amount (82.05 lakh) exceeds the trend estimation of (55.95). There was slight reduction in the amount involved in frauds in 2024-25 where, the actual amount was (73 lakh) with the trend value of (77.81), as compared to the amount involved in frauds in the year 2023-24 there is decrease of 11.3% in 2024-25.The amount involved in the cyber frauds in SBI has increased by more then 20% in the span of five years that is from 2020-21 to 2024-25.

FINDINGS AND DISCUSSION:

Sharp escalation in cyber fraud cases

The first major finding is the dramatic increase in the number of cyber fraud cases over the five year period. The data show that incidents were almost negligible at the beginning of the study but rose to several thousand cases by 2024-25. This pattern indicates that cyber fraud has shifted from a minor operational concern to a significant, recurring risk for the bank. This escalation to rapid growth in digital transactions, wider use of mobile and internet banking, and greater customer dependence on online channels. These developments expand the bank’s digital footprint and create more opportunities for attackers, especially where customers or staff have limited awareness of cyber security practices.

Rising financial impact of cyber frauds

The clear upward trend in the total amount involved in cyber frauds the table of “amount involved” shows that losses increasing substantially between 2020-21 and 2024-25 with the regression based trend values confirming a strong positive slope. This means that not only frauds are more frequent but each incident is also becoming more costly on average. This can be interpreted as evidence that fraudsters are targeting higher-value transactions, exploiting larger limits on digital channels, or benefiting from delays in detection and response. An increase in loss severity puts pressure on profitability, capital and reputation even when the absolute number of cases seems manageable.

Presence of abnormal spikes rather than smooth growth

The number of cases and the amount involved both do not grow smoothly they show pronounced spikes especially in 2023-24. In that year, the actual values for cases and amounts are far above the fitted trend line, indicating an abnormal surge beyond the underlying long run pattern. Major fraud incidents, exploitation of specific technological or procedural gaps or changes in reporting and classification that made more cases visible. This shows that cyber risk is not only increasing over time but can also putting stress on controls and investigation capacity in particular years.

Partial improvement but persistently high risk in the final year

The partial improvement observed in 2024-25, the data show a reduction in both the number of cases and the amount involved compared with the peak in 2023-24 and the actual loss in 2024-25 is slightly below the trend value. This suggests that strengthened monitoring, stricter controls and awareness programmes may have begun to moderate the impact of cyber frauds. The level in 2024-25 remain significantly higher than those in the early years of the study which means that the overall risk has stabilized at a higher base rather than returned to earlier low levels. While recent measures appear to be effective, they are not yet sufficient to reverse the upward trend and continuous improvement is required.

Tension between automation-driven growth and fraud vulnerability

The tension between SBI's successful automation and digital expansion and the simultaneous growth in cyber-fraud risk shows strong growth in customer base, digital usage and financial performance, while the empirical data highlight growing exposure to cyber incidents and losses. One could read the findings to suggest that automation and digitalisation deliver not only efficiency but also vulnerability. The lesson has to be that if you are going to spend all this money in digital distribution, you better at least spend the dollars on cybersecurity and fraud analytics, personnel capacity and customer education. If this balance is not in place, then the automation itself could actually be a lost cause due to fraud losses and customer trust impact from notifying them incorrectly.

CONCLUSION AND MANAGERIAL IMPLICATION

Conclusion

- Cyber Frauds across SBI Karnataka overall in a five-year span are seen to be rising with an increase in the number of fraud cases and also the total amount that people are losing.
- The long-run trend is clear from the (non-cumulative) fraud losses, extrapolating regular statistics 2023-24, appears to have been a peak, and 2024-25 a partial reverse.
- This trend would appear following the rise of increased surveillance, automated safeguards and proactive customer awareness efforts, though not enough to reverse cyber fraud back to historic lows akin to those experienced during the earlier stages of the study.
- The findings are in line with other national and international evidence to show that high transaction volumes, rapid digital take-up and sophisticated methods are contributing to fraud risk at big banks.
- If acquisition of SBI exercises is an objective, the results would challenge that one area of future eye focus around fraud risk management framework refreshment and not treating investment in cyber security, but others like advanced analytics and skill development to be considered as discretionary or peripheral spend.

Managerial implication

- Cyber security is a business issue to be addressed as part of the overall business strategy and enterprise risk, not a technical problem with limited relevance under the domain of IT alone.
- Senior management should monitor fraud incidents and losses through standard time series dashboards to catch new trends in the bud and to highlight outliers for investigation
- Such abnormal periods of peak fraud, like in 2023-24, require forensic reviews targeted and intense control testing around particular products, channels, transaction types and regions which have been the main cause behind such a surge.

- Reactive measures should include more resilient forms of authentication and implementation of enhanced real time monitoring rules while tightening the limits for high risk customer segments, combined with ways to bolster personnel background checks and access controls on sensitive positions.
- Ongoing customer and staff education is key as well, with fraud exercises to test knowledge/following procedures such as simulated attacks and guidance on how to bank securely online for customers - the best defence against phishing, social engineering or credential abuse.
- The bank, with regulators, industry groups and others, need to be working together in a proactive way, exchanging information about emerging fraud typologies red flag indicators of potential economic crime exposure, so that the bank can react more quickly to new cyber fraud schemes.

Limitations and future research directions

- The research relied on secondary data from five years and it dampens other long run cycles, structural breaks or seasonality in cyber fraud.
- The study is limited to the SBI, Karnataka. This is a constraint on generalisation, where the bank may be small or with different customer profile or product mix and systems infrastructure, but in other settings.
- Descriptive trends analysis across the strata using rate of change analysis of calendar on an aggregated level where ‘change’ is most readily visualised. It also doesn’t control for some other stuff that could easily muddle the explanation, such as transaction volume, channel and security controls mix and macro-economic factors.
- Estimates are for reported and detected fraud; there may be unreported or undetected fraud not included in these estimates. Well, we don’t know that yet in the cases not reported.

Future research direction

Future investigations should expand the time period on the other hand and apply more sophisticated techniques applied in time series to decompose trend effects from abrupt shocksand seasonal components that are used to detect cyber fraud.

- More generally, cross-bank, cross-region comparisons could show whether the SBI Karnataka trends are part of a system-wide phenomenon or if they are isolated weaknesses in banks.
- Increasing the levels of detail in our models, which could include more explanatory variables such as digital transaction volumes, product and channel mix, strength of controls applied to the risks and macroeconomic indicators, would allow for a clearer and robust mapping of drivers on cyber fraud incidence and loss.
- Mixed method designs, combining quantitative examination with interviews or case studies of bank managers, cyber-expert practitioners and victims, might explain corporate practices, operational weaknesses and systematic insights about behaviour antecedents which cause risk in banking 24-hour automated service against cyber fraud.

REFERENCES

1. Barik, T. r. (2025). 360 degree approach to cyber risk management as a strategic tool for fraud detection and prevention in banking . *The journal of indian institute of banking & finance* .

2. Bindhushree, M. (2024). the study of bank frauds cases and security controls in indian banking . *TIJER* , 11.

3. Kumar, A. (2022). impact of covid 19 on digital payment system in india . *IJIRT* .

4. kumar, m. (2024). a study on the financial performance of state bank of india in the post covid era with special reference to digital transformation . *international journal for multidisciplinary reserach* .

5. M, M. (2024). study on cyber frauds post digitalization in India . *International journal for research in applied science & engineering technology* .

6. Mehta, A. (2024). impact of technological advancements on banking frauds: A case study of indian banks . *international journal of research in finance and management* .

7. roy, D. (2024). bank frauds in india :Modus oprandi and preventive measures . *national institute of bank management* .

8. Chakrabarty, K. C. (2013). Governance failures in public sector banks and large-scale loan frauds: Recommendations for improvement. Journal of Banking Regulation, 14(2), 110–125. https://doi.org/10.1057/jbr.2013.

9. Gulpham, A. (2022). The inadequacies of India's judicial system in addressing financial fraud: Recommendations for stricter legal measures. Indian Journal of Law and Society, 13(1), 43–60.

10. Odeyemi, A., Okoye, L. U., & Ogundipe, A. (2024). Harnessing artificial intelligence for fraud detection in the banking sector: Opportunities and challenges. International Journal of Financial Studies, 12(1), 25–40. https://doi.org/10.3390/ijfs12010025

11. Mohan, V. (2023). Financial frauds in India: An overview of regulatory responses and future directions. Indian Journal of Banking and Finance, 12(2), 75–92.

12. Nair, S., & Sharma, T. (2021). The role of third-party audits in preventing banking fraud: Lessons from Indian public sector banks. Journal of Financial Regulation and Compliance, 29(4), 467–482.

13. Rathi, R., & Bhattacharya, A. (2023). Corporate governance and financial fraud in public sector banks: An empirical analysis. Journal of Business Ethics, 174(2), 367–382.

14. Singh, R. (2023). Systemic inefficiencies in public sector banks: A critical analysis of loan-related fraud. Journal of Financial Crime, 30(2), 234–248.