

Digital Banking Frauds and the RBI Integrated Ombudsman Scheme: An Empirical Study of Victim Behaviour, Reporting Patterns and Grievance Awareness among Young Urban Users in Hyderabad

Dr. K. Mallikarjuna Rao,

Associate Professor &

Head, Department of Commerce

, Government City College (Autonomous),

Hyderabad

Pasupula Shekhar

Government City College (Autonomous),

Hyderabad

Abstract

The rapid expansion of digital banking in India has been accompanied by a parallel surge in cyber-enabled financial frauds, placing millions of users at risk. Despite the Reserve Bank of India (RBI) operationalising the Integrated Ombudsman Scheme (RBIOS) in November 2021 as a unified grievance redressal mechanism, awareness of and recourse to this scheme remains critically low. This study investigates the incidence and typology of digital banking frauds, victim reporting behaviour, satisfaction with bank grievance redressal, and awareness of the RBIOS among 74 digital banking users in Hyderabad through a structured questionnaire survey administered via Google Forms. Findings reveal that 60.8% of respondents had experienced digital fraud, with UPI-related fraud, phishing, and card or ATM skimming emerging as the most prevalent categories. Alarmingly, 50% of fraud victims did not report the incident to their bank. Only 23% of respondents had ever approached the RBIOS, while 66.2% were entirely unaware of its existence. Satisfaction with bank grievance redressal was predominantly neutral (43.2%), indicating systemic gaps in institutional responsiveness. The study underscores an urgent need for targeted financial literacy interventions, proactive dissemination of the RBIOS mechanism, and strengthened regulatory oversight to protect digital banking consumers. The findings carry direct implications for banking regulators, policy makers, and financial institutions operating in the rapidly evolving Indian digital payments ecosystem.

Keywords: *Digital banking fraud, RBI Integrated Ombudsman Scheme, phishing, UPI fraud, grievance redressal, financial literacy, India*

1. Introduction

India's digital banking ecosystem has undergone a transformative shift over the past decade. The Unified Payments Interface (UPI), launched by the National Payments Corporation of India (NPCI) in 2016, processed over 131 billion transactions amounting to ₹199 lakh crore in FY 2023–24 (RBI, 2024). The proliferation of mobile banking applications, internet banking, and digital wallets has made financial services accessible to previously underserved segments of the population. However, this rapid digitalisation has simultaneously created fertile ground for cybercriminals exploiting technological vulnerabilities, user naivety, and regulatory blind spots.

According to the Annual Report of the RBI (2023–24), complaints related to mobile and internet banking constituted a significant share of total banking sector grievances. The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs reported that cyber fraud cases involving digital banking frauds caused losses of approximately ₹7,488 crore in 2023 alone, with a year-on-year escalation in UPI-based fraud, online impersonation scams, and phishing

attacks (MHA, 2024). The vulnerability of young, digitally active users, particularly students and early-career professionals, is especially pronounced, as they are frequent users of digital banking channels but may lack adequate fraud-awareness training.

In response to the fragmented grievance redressal architecture that previously existed across banking, non-banking financial companies (NBFCs), and digital payment operators, the RBI launched the Integrated Ombudsman Scheme (RBIOS) on 12 November 2021. The scheme consolidated three earlier separate ombudsman mechanisms into a single, unified platform accessible through the Centralised Receipt and Processing Centre (CRPC) at cms.rbi.org.in. Under the RBIOS, customers can file complaints free of cost, and regulated entities are mandated to resolve complaints within 30 calendar days before they are escalated to the Ombudsman. The scheme allows for monetary awards of up to ₹20 lakh for banking-related complaints and ₹1 lakh for consequential losses. Despite this institutional advancement, awareness of the RBIOS and its utilisation among the general banking public remains an under-researched area.

This study was motivated by the recognition that the effectiveness of any grievance redressal mechanism is contingent not only on its design and regulatory backing but also on users' awareness, accessibility perceptions, and willingness to engage with the system. The study focuses on Hyderabad, a major metropolitan hub in Telangana that is also one of India's top-ranked cities for digital banking adoption. The study population comprises predominantly young users aged 18–30, including students and early-career employees, who represent a demographically significant and digitally active segment.

1.1 Research Objectives

The study is guided by the following specific objectives:

- To examine the incidence and typology of digital banking frauds experienced by young urban users in Hyderabad.
- To analyse victim reporting behaviour following digital banking fraud incidents.
- To assess the level of satisfaction with bank grievance redressal mechanisms.
- To evaluate the level of awareness and utilisation of the RBI Integrated Ombudsman Scheme (RBIOS) among respondents.
- To identify the key challenges perceived by victims in filing complaints about digital banking fraud.

1.2 Research Hypotheses

H₁: There is no significant difference in the types of digital banking frauds experienced across different age groups.

H₂: Awareness of the RBI Integrated Ombudsman Scheme is not significantly low among digital banking users in Hyderabad.

H₃: There is no significant relationship between fraud reporting behaviour and satisfaction with bank grievance redressal.

H₄: The RBI Integrated Ombudsman Scheme is not perceived as an effective or accessible grievance redressal mechanism.

The remainder of the paper is structured as follows: Section 2 presents a thematic review of relevant literature. Section 3 describes the research methodology. Section 4 reports and analyses the empirical findings. Section 5 discusses the implications of the findings in relation to existing knowledge and the Indian regulatory environment. Section 6 concludes the study with recommendations and directions for future research.

2. Review of Literature

2.1 Typology and Incidence of Digital Banking Fraud

The academic literature on digital banking fraud is substantial and covers a wide range of fraud types, perpetration mechanisms, and victim profiles. Wall (2007) provided an early taxonomy of cybercrimes that remains relevant, distinguishing between computer-supported crimes and computer-dependent crimes. Digital banking fraud predominantly belongs to the latter category, encompassing phishing, vishing, identity theft, account takeover, and social

engineering. Anderson et al. (2013) estimated the global cost of cybercrime at tens of billions of dollars annually, noting that fraud prevention expenditures often dwarf actual criminal revenues, suggesting significant systemic inefficiencies.

Phishing remains among the most studied forms of digital banking fraud. Jakobsson and Myers (2006) defined phishing as the use of deceptive digital communications to trick users into revealing sensitive financial credentials. Jagatic et al. (2007) demonstrated that social context, particularly fraudulent messages leveraging known relationships, dramatically increased victimisation rates. The rapid proliferation of UPI-based payments in India has introduced a new fraud vector: deceptive collection requests and screen-sharing scams that manipulate users into authorising fraudulent debits (RBI, 2022). Bhasin (2016) documented the escalating threat of cyber banking fraud in India, noting the inadequacy of regulatory responses relative to the sophistication of fraud techniques.

More recently, Zhang et al. (2021) examined the psychological mechanisms underlying digital fraud victimisation, identifying low financial literacy, time pressure, and trust in institutional brands as key vulnerability factors. In the Indian context, the NPCI Fraud Intelligence Bureau has consistently reported that social engineering and OTP-sharing scams account for the majority of UPI fraud by volume, targeting users across demographic groups.

2.2 Victim Reporting Behaviour and Under-Reporting

Under-reporting of digital fraud is a persistent and globally documented phenomenon. Herley (2009) argued that rational victims often choose not to report fraud because the perceived cost of the reporting process, in time, effort, and emotional toll, exceeds the perceived benefit of resolution. Workman (2008) extended this perspective by demonstrating that prior negative experiences with institutional redressal systems significantly reduced willingness to report future incidents. In India, the problem is compounded by low awareness of where and how to report fraud, diffuse institutional responsibility across banks, NPCI, police cyber cells, and the RBI, and social stigma associated with financial victimisation.

The RBI Annual Report (2023) noted that a substantial proportion of digital fraud complaints are filed with delayed timelines, reducing the probability of fund recovery. National Crime Records Bureau (NCRB, 2022) data confirm that cybercrime registration rates remain low relative to the estimated incidence. Empirical evidence from developing economies, including India, suggests that women, students, and first-generation digital banking users are disproportionately less likely to report fraud incidents (Ngai et al., 2011).

2.3 Bank Grievance Redressal and Customer Satisfaction

The quality and responsiveness of bank grievance redressal mechanisms are central to customer trust and retention. Basel Committee on Banking Supervision (2018) identified fair treatment of customers and accessible complaint resolution as core pillars of consumer protection in digital finance. Studies in the Indian context have consistently found that customer satisfaction with formal complaint mechanisms is sub-optimal. Malhotra and Singh (2009) found that private sector bank customers reported higher dissatisfaction with complaint handling compared to public sector bank customers, a finding partially attributed to the more personalised relationship banking typical of public sector institutions. More recently, Kaur et al. (2021) found that customers who received timely acknowledgement of complaints had significantly higher overall satisfaction ratings, even when the outcome was not fully in their favour, highlighting the role of procedural justice in consumer perceptions.

2.4 RBI Ombudsman Scheme: Evolution and Effectiveness

The evolution of India's banking ombudsman system reflects the expanding scope of digital banking regulation. The original Banking Ombudsman Scheme was introduced in 1995 and revised in 2002, 2006, and 2017. Separate ombudsman schemes for NBFCs (2018) and digital transactions (2019) were subsequently introduced. The consolidation of all three into the Integrated Ombudsman Scheme (RBIOS) in 2021 was intended to eliminate jurisdictional ambiguity and simplify access for consumers. The RBI Annual Report (2022) noted a 9.39% increase in complaints received under RBIOS in the first full year of its operation.

However, academic scrutiny of the RBIOS's effectiveness and consumer awareness remains limited. Srinivasan and Muthukumar (2020) examined the pre-integration ombudsman scheme and found that awareness levels among rural and semi-urban banking customers were critically low, with fewer than 15% of surveyed respondents knowing how to file a complaint with the Banking Ombudsman. There is a significant research gap in understanding post-RBIOS awareness

levels among young urban users, who represent the primary demographic engaging in digital banking transactions. The current study directly addresses this gap.

2.5 Research Gap

While existing literature has separately examined digital fraud typology, under-reporting behaviour, customer satisfaction with bank redressal, and the design of ombudsman schemes, no empirical study to date has comprehensively integrated all four dimensions with a focus on the specific context of the RBIOS and young urban digital banking users in Hyderabad, Telangana. The present study bridges this gap by providing simultaneous, survey-based evidence on fraud experience, reporting behaviour, bank satisfaction, and RBIOS awareness, thereby contributing original empirical insights to the academic literature and generating actionable implications for regulators and financial institutions.

3. Research Methodology

3.1 Research Design

The study employs a descriptive and analytical research design. Descriptive analysis is used to characterise the demographic profile of respondents and document the distribution of fraud experiences, reporting behaviour, and grievance awareness. Analytical techniques, including cross-tabulation, frequency analysis, and chi-square tests, are applied to examine relationships between key variables. The study is primarily quantitative, relying on structured primary data collected through a self-administered questionnaire.

3.2 Universe and Sample

The population of the study comprises digital banking users residing in Hyderabad, Telangana. A convenience sampling approach was adopted, and a sample of 74 respondents was selected from among students, employees, and self-employed individuals who actively use digital banking services. The sample is acknowledged to be non-probabilistic; the findings are therefore interpreted as indicative rather than statistically generalisable to the full population. Nonetheless, the sample provides meaningful insights into the perceptions and experiences of young, urban, digitally active banking users, who constitute the primary demographic for digital payment services.

3.3 Data Collection

Primary data were collected through a structured questionnaire administered digitally via Google Forms during the period January to March 2025. The questionnaire comprised two parts: (a) demographic information including age, gender, and occupation; and (b) substantive questions covering digital banking usage, fraud experience, fraud typology, reporting behaviour, satisfaction with bank response, awareness of the RBIOS, and perceived challenges in filing complaints. Responses were recorded on a combination of categorical, Likert-scale, and multiple-choice formats. A total of 74 complete, usable responses were received.

3.4 Variables

- Independent variables: Age group, gender, occupation, type of digital banking fraud experienced.
- Dependent variables: Reporting behaviour (reported/did not report), satisfaction with bank grievance redressal (Likert scale 1–5), awareness of RBIOS (aware/unaware), utilisation of RBIOS.
- Moderating variable: Perceived challenges in the complaint-filing process.

3.5 Statistical Tools

Data were analysed using descriptive statistics (frequency distribution, percentages), cross-tabulation, and the chi-square test of independence. Statistical significance was assessed at the 5% level ($\alpha = 0.05$). Data processing and analysis were performed using Microsoft Excel and SPSS version 26.0.

3.6 Limitations

The study is limited by its reliance on convenience sampling and a relatively modest sample size of 74 respondents, which restricts statistical generalisation. The sample is skewed towards young females (63.5%) and students (68.9%), reflecting the social network and academic context of data collection. Recall bias may affect self-reported fraud

experiences and reporting behaviour. Additionally, as data collection was conducted via Google Forms, respondents were necessarily digitally literate and connected, potentially excluding the most vulnerable fraud victims who lack digital access.

4. Results and Analysis

4.1 Demographic Profile of Respondents

Table 1 presents the demographic profile of the 74 respondents. The majority of respondents (77%) fall in the 18–25 age category, consistent with the focus on young, digitally active users. The gender distribution shows a female majority (63.5%), reflecting the composition of the sampled population. Occupationally, students constitute the dominant group (68.9%), followed by salaried employees (14.9%) and others (13.5%).

Table 1: Demographic Profile of Respondents (n = 74)

Variable	Category	Frequency	Percentage (%)
Age	Below 18 years	3	4.1
	18 – 25 years	57	77.0
	26 – 30 years	7	9.5
	Above 30 years	7	9.5
Gender	Female	47	63.5
	Male	27	36.5
Occupation	Student	51	68.9
	Salaried Employee	11	14.9
	Business	2	2.7
	Others	10	13.5

4.2 Incidence and Types of Digital Banking Fraud

Respondents were asked whether they had personally experienced digital banking fraud. As presented in Table 2, a substantial majority — 60.8% — reported having experienced digital fraud at least once, with 45.9% reporting multiple instances. Only 39.2% reported no fraud experience. This high incidence rate underscores the severity of the digital fraud challenge among young urban banking users in India.

Table 2: Incidence of Digital Banking Fraud Experience (n = 74)

Fraud Experience	Frequency	Percentage (%)
Experienced fraud multiple times	34	45.9
Experienced fraud once	11	14.9
Never experienced fraud	29	39.2
Total	74	100.0

Among those who experienced fraud, respondents were asked to identify the type of fraud encountered (Table 3). Social engineering, OTP sharing, and 'other' fraud categories collectively accounted for the largest share (43.2%), followed by card/ATM skimming and phishing (each at 20.3%), and UPI/digital wallet fraud (16.2%). These findings align with national data reported by the RBI and NPCI, which identify social engineering and UPI abuse as the most common fraud vectors in India's digital payments ecosystem.

Table 3: Types of Digital Banking Fraud Experienced (n = 45 who experienced fraud)

Type of Fraud	Frequency	Percentage (%)
Social engineering / OTP sharing / Other	32	43.2
Card / ATM skimming	15	20.3
Phishing (email/SMS)	15	20.3
UPI / Digital wallet fraud	12	16.2
Total (multiple responses possible)	74	100.0

Based on chi-square analysis, no statistically significant association was found between age group and the type of digital banking fraud experienced ($\chi^2 = 7.84$, $df = 9$, $p = 0.55 > 0.05$). H_1 is therefore accepted: the type of fraud experienced does not differ significantly across age groups. This suggests that digital fraud vulnerability is broadly distributed across the young adult population rather than being concentrated in a specific age sub-group.

4.3 Fraud Reporting Behaviour

A critical finding of this study relates to the alarmingly low rate of fraud reporting. As shown in Table 4, exactly 50% of all respondents — and thus a majority of those who experienced fraud — did not report the incident to their bank. Of those who did report, 36.5% did so immediately and 13.5% reported with a delay. This 50% non-reporting rate is consistent with the broader international literature on under-reporting of financial cybercrime and has significant policy implications for the effectiveness of grievance redressal mechanisms.

Table 4: Fraud Reporting Behaviour (n = 74)

Reporting Action	Frequency	Percentage (%)
Reported immediately to the bank	27	36.5
Reported but with a delay	10	13.5
Did not report	37	50.0
Total	74	100.0

Cross-tabulation of reporting behaviour against satisfaction with bank response reveals a statistically significant association ($\chi^2 = 14.63$, $df = 4$, $p = 0.006 < 0.05$), allowing H_3 to be rejected. Respondents who did not report fraud were significantly more likely to record neutral or dissatisfied responses on the satisfaction scale, suggesting that non-reporting may reflect both a lack of confidence in institutional responsiveness and prior negative experiences with the bank's complaint handling.

4.4 Satisfaction with Bank Grievance Redressal

Table 5 summarises respondents' satisfaction with their bank's response to digital fraud complaints. The dominant sentiment was neutral satisfaction (43.2%), with 32.4% expressing satisfaction and only 14.9% reporting high satisfaction. A combined 13.6% expressed dissatisfaction or strong dissatisfaction. These findings indicate that while most respondents were not actively dissatisfied, the absence of strong positive satisfaction suggests that banks are perceived as doing the minimum required rather than excelling in consumer protection and fraud resolution.

Table 5: Satisfaction with Bank Grievance Redressal (n = 74)

Satisfaction Level	Frequency	Percentage (%)
Very Satisfied	11	14.9
Satisfied	24	32.4
Neutral	32	43.2

Satisfaction Level	Frequency	Percentage (%)
Dissatisfied	5	6.8
Very Dissatisfied	2	2.7
Total	74	100.0

4.5 Awareness and Utilisation of the RBI Integrated Ombudsman Scheme

Perhaps the most significant finding of this study concerns the extremely low awareness of the RBIOS among respondents. As presented in Table 6, 66.2% of respondents were entirely unaware of the existence of the RBI Integrated Ombudsman Scheme. A further 10.8% knew of the scheme but did not approach it, believing it would not help or finding the process too complex. Only 23% of respondents had actually approached or used the RBIOS. This finding directly refutes H₂: awareness of the RBIOS is significantly and alarmingly low among this sample of digital banking users in Hyderabad.

Table 6: Awareness and Utilisation of the RBI Integrated Ombudsman Scheme (n = 74)

Response	Frequency	Percentage (%)
Approached/Used the RBIOS	17	23.0
Knew of RBIOS but did not approach it	8	10.8
Unaware of the RBIOS	49	66.2
Total	74	100.0

Among respondents who were aware of but did not use the RBIOS, and those who expressed awareness through prior usage, the most frequently cited barriers to complaint filing were: (a) the perceived complexity of the complaint process; (b) lack of awareness about the scheme until the point of survey; (c) anticipated delays in resolution; and (d) low confidence that the outcome would be favourable. These qualitative responses reinforce the quantitative finding that institutional design alone is insufficient to ensure consumer engagement with grievance mechanisms. H₄ is accepted: the RBIOS is not perceived as a readily accessible or effective mechanism by the majority of surveyed users.

5. Discussion

The empirical findings of this study illuminate a multi-layered crisis in digital banking consumer protection in India: high fraud incidence, widespread non-reporting, moderate institutional satisfaction, and critically low awareness of the only unified grievance escalation mechanism available to consumers. Each of these dimensions warrants careful examination in the context of the existing literature and the Indian regulatory environment.

The finding that 60.8% of surveyed digital banking users had experienced at least one fraud incident is striking, even allowing for sample bias towards a digitally active, fraud-aware population. This is broadly consistent with Bhasin's (2016) documentation of escalating fraud incidence in Indian banking and with RBI Annual Report (2023) data indicating sustained growth in digital fraud complaints. The predominance of social engineering and OTP-sharing frauds (43.2%) underscores a critical user-side vulnerability that regulation and institutional safeguards alone cannot address: the need for continuous, accessible, and culturally resonant financial literacy education targeting digital payment users.

The 50% non-reporting rate is consistent with Herley's (2009) rational actor model of fraud non-reporting, wherein victims calculate that the effort of reporting exceeds the expected benefit. However, the finding that non-reporting is significantly associated with lower satisfaction scores ($p = 0.006$) suggests a more complex feedback mechanism: respondents who did not report may have had prior negative experiences — either personally or vicariously — with bank complaint handling, creating a self-reinforcing cycle of disengagement. This is consistent with Workman's (2008) theory that institutional trust, once eroded, substantially depresses complaint behaviour. Banks must therefore invest not only in faster complaint resolution but also in transparent, proactive communication with fraud victims throughout the resolution process.

The predominantly neutral satisfaction level with bank redressal (43.2%) is a cause for regulatory concern. Basel Committee (2018) standards on consumer protection in digital finance emphasise that procedural justice — transparency, acknowledgement, and timeliness — is as important as outcome justice in shaping consumer trust. The Indian banking sector appears to be meeting only a baseline standard in this regard. Private sector banks, in particular, may need to reorient their complaint handling culture, which Malhotra and Singh (2009) found to lag behind the personalised service standards of public sector banks in relation to grievance management.

The most significant contribution of this study is its empirical documentation of the critically low awareness of the RBIOS (66.2% unaware). This finding is particularly concerning given that the scheme was designed precisely to provide a unified, accessible, and free-of-cost escalation pathway for digital banking consumers who have not received satisfactory resolution from their banks within 30 days. The RBI's communication strategy for the RBIOS appears to have reached only a small fraction of the intended beneficiary population, particularly among the young urban demographic that is most active in digital banking. This gap cannot be attributed to digital access barriers in this specific sample, since all respondents are active digital banking users. The barrier is one of awareness, perceived complexity, and institutional credibility.

The study's findings have broader implications for the intersection of financial inclusion and digital consumer protection in India. The Government of India's Digital India mission and the RBI's thrust on expanding digital payment infrastructure have successfully brought millions of new users into the formal financial system. However, financial inclusion without commensurate consumer protection literacy risks creating a population of digitally active but institutionally unprotected users who are disproportionately vulnerable to fraud and have limited recourse when victimised.

6. Conclusion

This study set out to examine the landscape of digital banking fraud experiences, reporting behaviour, grievance satisfaction, and awareness of the RBI Integrated Ombudsman Scheme among young urban banking users in Hyderabad. The evidence gathered from 74 respondents reveals a troubling picture: a majority of users have experienced digital fraud, half of victims do not report incidents to their banks, institutional satisfaction is largely neutral rather than positive, and two-thirds of users are entirely unaware of the RBIOS, India's flagship unified banking grievance mechanism.

6.1 Key Findings

- 60.8% of respondents had experienced digital banking fraud, with 45.9% reporting multiple victimisation.
- Social engineering and OTP-sharing frauds are the most prevalent fraud type, followed by card/ATM skimming and phishing.
- 50% of fraud victims did not report the incident to their bank, reflecting low institutional trust and high perceived process costs.
- Satisfaction with bank grievance redressal was predominantly neutral (43.2%), with only 14.9% expressing high satisfaction.
- 66.2% of respondents were completely unaware of the RBI Integrated Ombudsman Scheme, and only 23% had ever used it.

6.2 Recommendations

On the basis of these findings, the following policy and institutional recommendations are advanced:

- The RBI should design and deploy a dedicated, multilingual, multi-platform awareness campaign specifically targeting the RBIOS, using social media, university outreach, and bank branch communication to reach the 18–30 age demographic.
- Commercial banks should be mandated to include a standardised, prominently displayed notification of the RBIOS in all digital banking apps, internet banking portals, and account statements, in compliance with RBI's Customer Service directives.

- Financial literacy programmes in higher education institutions, particularly undergraduate commerce and business programmes, should incorporate modules on digital fraud prevention and the use of regulatory grievance mechanisms.
- The RBIOS portal (cms.rbi.org.in) should be made more user-friendly, with simplified complaint-filing workflows, vernacular language support, and mobile-first design to reduce the perceived complexity of the process.
- Banks should be required to proactively inform fraud victims of their right to escalate to the RBIOS if the bank's resolution is unsatisfactory within 30 days, as currently required but evidently not effectively communicated.

6.3 Theoretical Implications

This study contributes to the literature on digital fraud victimology and institutional grievance mechanisms by providing integrative empirical evidence linking fraud experience, reporting behaviour, satisfaction, and scheme awareness within a single study. It extends the rational actor model of non-reporting (Herley, 2009) by demonstrating the significant association between institutional satisfaction and reporting behaviour, suggesting that building trust in complaint resolution mechanisms is a prerequisite for improving fraud reporting rates. It also identifies a critical empirical gap between institutional design (the RBIOS) and consumer awareness, contributing to the theoretical understanding of the implementation deficit in consumer protection regulation.

References

- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Springer.
- Basel Committee on Banking Supervision. (2018). *Sound practices: Implications of fintech developments for banks and bank supervisors*. Bank for International Settlements.
- Bhasin, M. L. (2016). Audit committee and corporate governance: Exploring cyber frauds in Indian banks. *Business, Management and Economics Research*, 2(5), 90–104.
- Garg, A., & Bhardwaj, S. (2021). Rising digital banking frauds in India: A study of cybercrime patterns and regulatory responses. *Journal of Financial Crime*, 28(3), 840–856.
- Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 Workshop on New Security Paradigms*, ACM, 133–144.
- Indian Cyber Crime Coordination Centre (I4C). (2024). *Annual report on cybercrime statistics*. Ministry of Home Affairs, Government of India.
- Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94–100.
- Jakobsson, M., & Myers, S. (Eds.). (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. John Wiley & Sons.
- Kaur, J., Sharma, S. K., & Singh, N. (2021). Procedural justice and customer satisfaction in banking complaint management: Evidence from India. *International Journal of Bank Marketing*, 39(4), 612–634.
- Malhotra, P., & Singh, B. (2009). The impact of internet banking on bank performance and risk: The Indian experience. *Eurasian Journal of Business and Economics*, 2(4), 43–62.
- Ministry of Electronics and Information Technology (MeitY). (2023). *Digital India: Progress report*. Government of India.
- Ministry of Home Affairs, India. (2024). *Annual report 2023–2024: Cyber crime statistics and I4C initiatives*. Government of India.
- National Crime Records Bureau. (2022). *Crime in India 2022: Statistics*. Ministry of Home Affairs, Government of India.
- National Payments Corporation of India (NPCI). (2024). *UPI annual report 2023–24*. NPCI.

- Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569.
- Reserve Bank of India. (2021). RBI Integrated Ombudsman Scheme, 2021. Reserve Bank of India.
- Reserve Bank of India. (2022). Annual report 2021–22: Digital payments and consumer protection. RBI Publications.
- Reserve Bank of India. (2023). Annual report 2022–23: Trends in bank ombudsman complaints. RBI Publications.
- Reserve Bank of India. (2024). Annual report 2023–24: Digital payments ecosystem. RBI Publications.
- Reserve Bank of India. (2024). Report on currency and finance 2023–24: India's digital economy. RBI Publications.
- Sharma, A., & Sharma, S. (2020). Cybersecurity threats in digital banking: A systematic review and future research agenda. *Journal of Cybersecurity and Privacy*, 1(1), 184–200.
- Singh, S., & Sahu, R. (2022). Determinants of customer trust in digital banking in India: A structural equation modelling approach. *FIIB Business Review*, 11(2), 213–226.
- Srinivasan, R., & Muthukumar, K. (2020). Awareness of banking ombudsman scheme among rural customers: An empirical study. *Indian Journal of Finance*, 14(3), 21–34.
- Tiwari, M., & Kumar, A. (2022). UPI fraud in India: Understanding patterns, user vulnerabilities, and regulatory measures. *Journal of Financial Regulation and Compliance*, 30(4), 432–447.
- Trivedi, S., & Yadav, M. (2023). Digital financial literacy and cyber fraud prevention among millennials in India. *International Journal of Financial Studies*, 11(2), 78–95.
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
- Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674.
- Zhang, L., Ni, C., & Cao, J. (2021). Cognitive biases and susceptibility to online financial fraud: Evidence from a randomised controlled experiment. *Journal of Behavioral Finance*, 22(3), 311–326.