International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Banking Frauds in India: A Comparative Legal Study of Rajasthan and Other States

Dr. Renu Vijaywargia

Assistant Professor, Bhagwan Mahaveer Law College and Research Centre

Abstract

The rapid expansion of digital banking in India has significantly enhanced financial inclusion, convenience, and accessibility of banking services. However, the increasing reliance on digital platforms has simultaneously led to a substantial rise in cyber-enabled financial crimes and digital banking frauds. These frauds include phishing, vishing, identity theft, unauthorized electronic fund transfers, UPI-related scams, and online payment frauds, posing serious challenges to consumers, financial institutions, and regulatory authorities. This study undertakes a comparative legal analysis of digital banking frauds in Rajasthan and selected Indian states to examine the effectiveness of existing legal and regulatory mechanisms in addressing such offences. The research critically evaluates the legal framework governing digital banking frauds, including specific provisions of the Information Technology Act, 2000 (Sections 43, 66, 66C, 66D, and 72A), the Bharatiya Nyaya Sanhita, 2023 (Sections 316, 318, 319, and 336), the Digital Personal Data Protection Act, 2023, Reserve Bank of India guidelines, and state-level cybercrime enforcement mechanisms. It further analyses patterns of digital banking fraud, reporting mechanisms, investigation procedures, victim compensation policies, and judicial responses across different jurisdictions, drawing on recent case law including State Bank of India v. Pallabh Bhowmick and Justice K. S. Puttaswamy v. Union of India. Particular emphasis is placed on a quantitative and institutional comparison of Rajasthan's cybercrime prevention initiatives, including the proposed Rajasthan Cyber Crime Coordination Centre (R4C), against the comparative effectiveness of Telangana, Karnataka, Maharashtra, and Uttar Pradesh, which report the highest cybercrime volumes nationally. The study identifies key legal and procedural gaps affecting the prevention, detection, and prosecution of digital banking frauds. It highlights the need for enhanced inter-agency coordination, stronger consumer protection measures, technological safeguards, and greater public awareness. The findings contribute to the ongoing discourse on strengthening India's cyber-financial security framework and offer recommendations for developing a more robust and uniform legal response to digital banking frauds across states.

Keywords: Digital Banking Fraud, Cybercrime, Information Technology Act, Bharatiya Nyaya Sanhita, Data Privacy, Digital Personal Data Protection Act, Consumer Protection, Cyber Law, Rajasthan.

1. Introduction

Digital banking has become one of the most significant developments in the Indian financial sector, transforming the manner in which banking services are accessed, delivered, and regulated. The integration of digital technologies into banking operations has enabled customers to perform financial transactions without visiting physical branches, thereby enhancing efficiency, convenience, and accessibility. India's

transition towards digital banking has been supported by rapid technological advancement, increasing internet penetration, and proactive governmental initiatives aimed at promoting financial inclusion. The banking industry has witnessed a paradigm shift from traditional service delivery mechanisms to technology-driven platforms that facilitate real-time transactions and remote banking services. As a result, digital banking has become an integral component of the country's economic modernization and financial governance framework. The growing dependence on electronic channels for financial transactions has not only expanded banking outreach but has also introduced new legal and security challenges. Consequently, understanding the evolution and implications of digital banking has become essential for legal scholars, policymakers, and financial regulators seeking to ensure the secure functioning of the digital financial ecosystem (Reserve Bank of India [RBI], 2024; World Bank, 2023).

The remarkable growth of digital banking in India can be attributed to a combination of policy reforms, technological innovation, and changing consumer behavior. Government initiatives such as Digital India, Pradhan Mantri Jan Dhan Yojana, and the promotion of cashless transactions have significantly contributed to expanding the digital banking infrastructure across urban and rural areas. The widespread adoption of smartphones and affordable internet services has enabled millions of individuals to access banking facilities through digital platforms. Furthermore, financial institutions have increasingly invested in digital transformation strategies to improve customer experience and operational efficiency. The COVID-19 pandemic further accelerated the adoption of digital banking as consumers sought contactless methods of conducting financial transactions. This unprecedented growth has strengthened financial inclusion by bringing previously unbanked populations into the formal financial system. However, the rapid expansion of digital banking services has also increased the exposure of users to cyber risks and financial frauds, necessitating a careful examination of the legal safeguards governing digital financial transactions (International Monetary Fund [IMF], 2023; RBI, 2024).

A defining feature of India's digital banking revolution has been the emergence of advanced digital payment systems such as Unified Payments Interface (UPI), Internet Banking, Mobile Banking, Immediate Payment Service (IMPS), National Electronic Funds Transfer (NEFT), and digital wallets. Among these innovations, UPI has emerged as a globally recognized payment system due to its simplicity, interoperability, and ability to facilitate instant fund transfers. These technologies have transformed consumer behavior by enabling seamless and convenient financial transactions through mobile devices and internet-enabled platforms. Businesses, government agencies, and consumers increasingly rely on digital payment mechanisms for commercial transactions, utility payments, and financial management. The success of these systems has significantly contributed to reducing cash dependency and promoting a digitally integrated economy. Nevertheless, the widespread use of digital payment platforms has also created new opportunities for cybercriminals to exploit technological vulnerabilities and human errors. As digital payment ecosystems continue to evolve, ensuring their security and reliability remains a critical challenge for regulators and financial institutions (National Payments Corporation of India [NPCI], 2024; World Economic Forum, 2023).

Despite the numerous benefits associated with digital banking, India has witnessed a substantial rise in digital banking frauds and cyber-financial crimes. Fraudsters increasingly employ sophisticated techniques such as phishing, vishing, identity theft, SIM-swapping, malware attacks, and fraudulent UPI transactions to gain unauthorized access to financial accounts. These crimes often exploit gaps in cybersecurity awareness among users and weaknesses within digital infrastructures. The financial losses resulting from such fraudulent activities have affected individuals, businesses, and banking institutions

across the country. Moreover, digital banking frauds have broader implications beyond financial harm, including psychological distress, erosion of consumer confidence, and reputational damage to financial institutions. The increasing complexity and transnational nature of cyber-financial crimes have further complicated efforts to investigate and prosecute offenders effectively. Consequently, digital banking fraud has emerged as a critical challenge requiring coordinated responses from regulators, law enforcement agencies, financial institutions, and consumers. The growing prevalence of cyber-enabled financial offences underscores the urgent need for robust legal mechanisms capable of addressing evolving technological threats (Ministry of Home Affairs, 2024; United Nations Office on Drugs and Crime [UNODC], 2023).

The rise of digital banking frauds has generated significant legal concerns regarding consumer protection, cybersecurity, institutional accountability, and the administration of justice. Traditional legal frameworks governing fraud and financial misconduct were primarily designed for conventional banking environments and often struggle to address the complexities of technology-driven offences. Digital financial crimes frequently involve issues of cross-border jurisdiction, electronic evidence, data privacy, and attribution of liability. Consequently, regulators and policymakers have recognized the need to modernize legal frameworks to address emerging cyber threats effectively. Various legislative measures, regulatory guidelines, and judicial interventions have sought to strengthen the legal response to digital banking frauds. Nevertheless, challenges persist in ensuring timely investigation, effective prosecution, and adequate compensation for victims. The dynamic nature of cybercrime requires legal systems to remain adaptable and responsive to technological developments. Therefore, a critical examination of existing laws and regulatory mechanisms is essential for assessing their effectiveness in protecting consumers and maintaining confidence in digital financial systems (Kumar & Sharma, 2022; RBI, 2024).

The increasing dependence on digital banking services highlights the necessity of comprehensive legal and regulatory intervention to safeguard the integrity of India's financial ecosystem. Effective governance of digital banking requires a multi-dimensional approach encompassing technological safeguards, legal accountability, consumer awareness, and institutional coordination. Regulatory authorities must continuously update cybersecurity standards and fraud prevention mechanisms to address emerging risks. Simultaneously, financial institutions must invest in advanced security technologies and user education programs to minimize vulnerabilities. Comparative legal analysis can provide valuable insights into best practices adopted by different jurisdictions in combating digital banking frauds. Such analysis is particularly relevant in the Indian context, where variations in technological infrastructure, digital literacy, and enforcement capacity influence the effectiveness of fraud prevention strategies. Ultimately, strengthening the legal framework governing digital banking frauds is essential not only for protecting consumers but also for ensuring the long-term sustainability and credibility of India's digital economy. This study therefore seeks to examine the phenomenon of digital banking fraud through a comparative legal analysis of Rajasthan and other Indian states, with the objective of identifying challenges, evaluating legal responses, and proposing policy reforms (Organisation for Economic Co-operation and Development [OECD], 2023; World Bank, 2023).

2. Conceptual Framework of Digital Banking Frauds

Digital banking fraud refers to any unauthorized, deceptive, or illegal activity conducted through electronic banking channels with the intention of obtaining financial gain or causing financial loss to another person or institution. Unlike conventional banking frauds, digital banking frauds are facilitated

through technological platforms such as internet banking, mobile applications, payment gateways, and electronic transaction systems. The nature of digital banking fraud is dynamic because offenders continuously adapt their methods in response to technological advancements and security improvements. Digital frauds often involve manipulation of personal information, unauthorized access to accounts, and misuse of digital credentials. The virtual nature of such crimes makes them difficult to detect and investigate, particularly when perpetrators conceal their identities through sophisticated technological means. Furthermore, digital banking frauds frequently transcend geographical boundaries, creating jurisdictional challenges for law enforcement agencies. The increasing reliance on digital transactions has expanded opportunities for cybercriminals to exploit vulnerabilities within technological systems and human behavior. Consequently, digital banking fraud is not merely a financial offence but also a significant cybersecurity and legal concern that affects the stability of the digital financial ecosystem. Understanding the conceptual foundations of digital banking fraud is essential for developing effective legal and regulatory responses capable of addressing emerging technological risks (Bhasin, 2022; Reserve Bank of India [RBI], 2024).

The evolution of digital banking has created an environment where fraud can occur through multiple channels and techniques. One of the most common forms of digital banking fraud is phishing, which involves fraudulent emails, messages, or websites designed to deceive individuals into disclosing sensitive information such as passwords, banking credentials, or one-time passwords (OTPs). Cybercriminals frequently imitate legitimate institutions to gain the trust of victims and induce them to reveal confidential information. Phishing attacks have become increasingly sophisticated due to advancements in social engineering techniques and digital communication technologies. In many cases, victims are unaware that they are interacting with fraudulent entities until unauthorized transactions have already occurred. The effectiveness of phishing schemes often depends on exploiting human psychology rather than technological weaknesses alone. Consequently, consumer awareness and digital literacy have become crucial components of fraud prevention strategies. Financial institutions continuously invest in cybersecurity measures to counter phishing attacks; however, the persistent adaptability of cybercriminals presents ongoing challenges. The prevalence of phishing underscores the importance of integrating technological safeguards with educational initiatives aimed at enhancing consumer vigilance and reducing susceptibility to deceptive practices (Kshetri, 2023; Ministry of Home Affairs, 2024).

Another significant category of digital banking fraud includes vishing, SIM-swap fraud, and identity theft. Vishing, or voice phishing, involves fraudsters impersonating bank officials, government representatives, or customer service personnel through telephone communications to obtain confidential financial information. Victims are often persuaded to disclose account details, OTPs, or card information under the false belief that they are communicating with legitimate authorities. SIM-swap fraud occurs when criminals fraudulently obtain control of a victim's mobile phone number by manipulating telecommunication service providers. Once access is secured, perpetrators can intercept authentication messages and gain unauthorized access to banking accounts. Identity theft involves the unauthorized acquisition and misuse of personal information for fraudulent financial transactions. The increasing availability of personal data through digital platforms has facilitated the growth of identity-related crimes. These forms of fraud highlight the interconnected nature of telecommunications, digital identity systems, and banking infrastructure. Effective prevention requires collaboration among banks, telecommunication providers, regulatory agencies, and consumers. The legal implications of these offences extend beyond financial loss and encompass issues of privacy, data protection, and digital security (Organisation for

Economic Co-operation and Development [OECD], 2023; United Nations Office on Drugs and Crime [UNODC], 2023).

The rapid adoption of Unified Payments Interface (UPI) and mobile banking applications has introduced new forms of fraud specifically targeting digital payment systems. UPI-related frauds commonly involve fake payment requests, QR code manipulation, fraudulent customer support services, and unauthorized transaction authorization. Cybercriminals exploit users' limited understanding of digital payment processes to induce them into approving transactions that benefit the perpetrators. Malware attacks represent another significant threat to digital banking security. Malicious software may be installed on a victim's device through infected links, fraudulent applications, or compromised websites. Once installed, malware can capture login credentials, monitor user activity, and facilitate unauthorized access to financial accounts. The increasing sophistication of malware technologies has made detection and prevention more challenging for both consumers and financial institutions. As digital payment systems continue to expand, the complexity of associated fraud risks also increases. Consequently, technological innovation must be accompanied by continuous investment in cybersecurity infrastructure and regulatory oversight to ensure the integrity and reliability of digital financial services (National Payments Corporation of India [NPCI], 2024; World Economic Forum, 2023).

Several factors contribute to the increasing prevalence of digital financial crimes in India. The rapid expansion of digital banking services has significantly increased the number of potential targets available to cybercriminals. Simultaneously, varying levels of digital literacy among consumers create opportunities for exploitation through deceptive practices and social engineering techniques. The growing use of interconnected digital platforms has also increased the potential impact of cybersecurity breaches. Inadequate cybersecurity measures, weak password practices, delayed software updates, and limited awareness regarding online security further exacerbate vulnerabilities. Economic motivations remain a primary driver of cybercrime, as digital banking fraud often provides substantial financial rewards with relatively low risks of detection. Furthermore, the anonymity afforded by digital networks enables offenders to conceal their identities and operate across multiple jurisdictions. The convergence of technological accessibility, economic incentives, and human vulnerabilities has contributed to the rapid growth of cyber-financial crimes throughout India. Understanding these causal factors is essential for developing targeted prevention strategies and strengthening institutional resilience against emerging threats (International Telecommunication Union [ITU], 2023; World Bank, 2023).

The impact of digital banking fraud extends far beyond immediate financial losses experienced by individual victims. Consumers often suffer emotional distress, loss of confidence in digital financial systems, and concerns regarding the security of personal information. Vulnerable populations, including senior citizens and first-time digital banking users, may be particularly affected by fraudulent activities. Financial institutions also face significant consequences, including reputational damage, increased compliance costs, operational disruptions, and legal liabilities. The cumulative effect of digital banking fraud can undermine public trust in the broader digital economy and discourage the adoption of innovative financial technologies. From a regulatory perspective, widespread cyber-financial crimes place additional pressure on law enforcement agencies, judicial institutions, and financial regulators responsible for maintaining system integrity. Therefore, digital banking fraud represents a multidimensional challenge affecting economic development, consumer protection, cybersecurity governance, and legal enforcement. Addressing these consequences requires a coordinated approach that combines technological innovation,

legal reform, public awareness, and institutional cooperation to create a secure and trustworthy digital financial environment (International Monetary Fund [IMF], 2023; RBI, 2024).

3. Legal and Regulatory Framework Governing Digital Banking Frauds

The legal framework governing digital banking frauds in India has evolved significantly in response to technological advancements and the increasing prevalence of cyber-enabled financial crimes. One of the foundational statutes addressing digital offences is the Information Technology Act, 2000, which provides legal recognition to electronic transactions and establishes a framework for addressing cybercrime. The Act contains provisions dealing with unauthorized access, identity theft, data theft, computer-related offences, and electronic fraud. Several specific provisions have become particularly relevant to digital banking fraud. Section 43 imposes civil liability and compensation for unauthorized access to, or damage caused to, a computer, computer system, or computer network, and is frequently invoked where a victim's banking credentials are accessed without authorization. Section 66 criminalizes the acts covered under Section 43 where committed dishonestly or fraudulently, attracting imprisonment of up to three years or a fine of up to five lakh rupees, or both. Section 66C specifically penalizes identity theft, that is, the fraudulent or dishonest use of another person's electronic signature, password, or other unique identification feature, while Section 66D penalizes cheating by personation through a computer resource or communication device, a provision regularly applied to phishing, vishing, and fraudulent UPI-collect-request cases. Both Sections 66C and 66D carry punishment of imprisonment up to three years together with a fine of up to one lakh rupees. Section 72A further penalizes the disclosure of personal information in breach of a lawful contract, with imprisonment of up to three years or a fine of up to five lakh rupees, a provision of particular relevance where bank or payment-intermediary employees wrongfully disclose customer data that is subsequently used to perpetrate fraud. The Information Technology Act also recognizes electronic records and digital signatures, thereby facilitating secure digital transactions. Over the years, amendments to the legislation have sought to strengthen cybersecurity provisions and address emerging technological challenges. Despite its significance, scholars have argued that the Act requires continuous updating to effectively respond to evolving cybercrime methodologies. Nevertheless, the Information Technology Act remains a critical component of India's legal response to digital banking fraud and cyber-financial offences (Government of India, 2000/2008; Sharma & Gupta, 2022).

The enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS) represents a significant development in India's criminal justice framework. Replacing several provisions of the former Indian Penal Code, the BNS incorporates offences that are increasingly relevant to the digital environment, including cheating, forgery, impersonation, and fraudulent misrepresentation conducted through electronic means. Although cybercrime-specific provisions continue to be addressed through specialized legislation such as the Information Technology Act, the BNS provides important substantive criminal law provisions that may be invoked in cases involving digital banking fraud. Most digital banking fraud prosecutions invoke Section 318 BNS (corresponding to the erstwhile Sections 415, 417, and 420 of the Indian Penal Code), which defines and punishes cheating, including the dishonest inducement of a victim to part with money or property, with imprisonment of up to seven years depending on the gravity of the offence. Where a fraudster impersonates a bank official or another individual to induce the transfer of funds, Section 319 BNS (replacing Section 419 of the Indian Penal Code) on cheating by personation applies, carrying imprisonment of up to five years. Section 316 BNS (replacing Sections 405 to 409 of the Indian Penal Code) addresses criminal breach of trust and is relevant where a person in a position of trust, such as a

bank employee or agent, dishonestly misappropriates entrusted funds, with enhanced punishment of up to ten years where the offender is a banker or public servant. Section 336 BNS (replacing Sections 463 to 471 of the Indian Penal Code) penalizes forgery, including the creation of false electronic records, which frequently accompanies fabricated KYC documents or forged payment instructions used to perpetrate digital banking fraud. Offences involving deception, dishonest inducement, and unlawful gain frequently overlap with cyber-enabled financial crimes. Consequently, the BNS serves as an important complementary framework supporting the prosecution of digital banking offenders. The incorporation of modernized criminal law principles reflects an acknowledgment of changing patterns of criminal activity in an increasingly digital society. Effective enforcement, however, depends upon coordination between traditional criminal law mechanisms and specialized cybercrime legislation. This integration is essential for ensuring comprehensive legal accountability for offenders operating within digital financial environments (Government of India, 2023; Singh, 2024).

The Reserve Bank of India plays a central role in regulating digital banking and mitigating fraud risks through its regulatory and supervisory functions. RBI regularly issues guidelines, circulars, and directions concerning cybersecurity, customer protection, electronic banking security, and fraud reporting. These regulatory instruments establish obligations for banks regarding risk management, customer authentication, transaction monitoring, and incident response. RBI has introduced measures such as two-factor authentication, real-time transaction alerts, and zero-liability protections for customers under specified circumstances. Additionally, banks are required to implement robust cybersecurity frameworks and maintain mechanisms for detecting suspicious transactions. RBI's emphasis on consumer awareness campaigns has further contributed to strengthening fraud prevention efforts. The dynamic nature of cyber threats necessitates continuous regulatory adaptation, and RBI has demonstrated an ongoing commitment to updating its guidelines in response to emerging risks. Through its supervisory authority, RBI plays a pivotal role in maintaining public confidence in digital banking systems and promoting secure financial transactions across the country (Reserve Bank of India, 2024; RBI, 2023).

Consumer protection has emerged as a critical aspect of the legal framework governing digital banking frauds. The Consumer Protection Act, 2019 provides important safeguards for consumers who suffer losses resulting from unfair trade practices, deficient services, or misleading representations. Digital banking users may seek remedies under consumer protection law when financial institutions fail to exercise reasonable care in providing secure banking services, particularly under Section 2(11) of the Act, which defines “deficiency in service” and has been the basis on which consumer fora and courts have held banks liable for failing to prevent or promptly redress unauthorized digital transactions. Banks are additionally subject to the regulatory and supervisory powers of the Reserve Bank of India under Section 35A of the Banking Regulation Act, 1949, which empowers RBI to issue binding directions in the interest of banking policy and depositor protection, including directions on digital payment security. The Act recognizes electronic commerce and digital transactions, thereby extending consumer rights into the digital environment. Consumer commissions have increasingly addressed disputes involving unauthorized transactions, deficient grievance redressal mechanisms, and negligence in maintaining cybersecurity standards. The emphasis on consumer welfare reflects the recognition that individuals often possess limited bargaining power and technical expertise when dealing with complex digital systems. By providing accessible remedies and compensation mechanisms, consumer protection law complements other regulatory measures aimed at combating digital banking fraud. Consequently, the Consumer Protection

Act serves as an important instrument for promoting accountability and protecting consumer interests within the digital financial ecosystem (Consumer Protection Act, 2019; Nair, 2023).

The Indian Computer Emergency Response Team (CERT-In) constitutes a vital institutional mechanism for addressing cybersecurity incidents and enhancing digital resilience. Established under the Information Technology Act, CERT-In functions as the national agency responsible for coordinating responses to cybersecurity incidents, issuing advisories, facilitating information sharing, and promoting cybersecurity best practices. In the context of digital banking fraud, CERT-In plays a crucial role in identifying emerging threats, disseminating threat intelligence, and supporting incident response efforts. Financial institutions frequently rely on CERT-In advisories to strengthen cybersecurity measures and address vulnerabilities. The agency's collaborative approach encourages cooperation among government departments, private sector organizations, and international stakeholders. Through capacity-building initiatives and technical guidance, CERT-In contributes significantly to India's broader cybersecurity governance framework. As cyber threats become increasingly sophisticated, the importance of institutional mechanisms such as CERT-In continues to grow. Effective collaboration between CERT-In, financial regulators, and law enforcement agencies is essential for strengthening national resilience against cyber-financial crimes (CERT-In, 2024; Ministry of Electronics and Information Technology, 2023).

An equally important component of the regulatory framework is the development of cybercrime reporting and grievance redressal mechanisms. The National Cyber Crime Reporting Portal and the Cyber Crime Helpline (1930) provide accessible platforms through which victims can report incidents of digital fraud and seek assistance. These mechanisms facilitate timely intervention by law enforcement agencies and improve the prospects of recovering fraudulently transferred funds. State cybercrime units, specialized police stations, and digital forensic laboratories further contribute to investigative and enforcement efforts. The effectiveness of reporting mechanisms depends largely on public awareness, institutional responsiveness, and inter-agency coordination. Delays in reporting often reduce the likelihood of successful intervention and asset recovery. Consequently, regulatory authorities have emphasized the importance of prompt reporting and public education campaigns. Strengthening cybercrime reporting infrastructure is essential for improving victim support, enhancing investigative outcomes, and promoting accountability within the digital financial ecosystem. Together, these legal and institutional mechanisms form the foundation of India's response to digital banking fraud and cyber-financial crime (Ministry of Home Affairs, 2024; UNODC, 2023).

3.1 Judicial Pronouncements on Digital Banking Fraud, Bank Liability, and Privacy

The statutory framework discussed above has been substantially shaped and clarified through judicial interpretation. In State Bank of India v. Pallabh Bhowmick & Ors. (SLP No. 30677 of 2024, decided on January 3, 2025), the Supreme Court dismissed SBI's challenge to a Gauhati High Court ruling and held that a customer who promptly reports an unauthorized online transaction cannot be saddled with liability where no negligence on the customer's part is established, applying Clauses 8 and 9 of the RBI Circular dated July 6, 2017 on Customer Protection—Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. The Court emphasized that banks must adopt robust technological measures to detect and prevent fraudulent transactions and cannot abdicate this responsibility merely because a customer enters a correct one-time password. The Delhi High Court reached a similarly protective conclusion in Hare Ram Singh v. Reserve Bank of India (W.P.(C) 13497/2022, decided on November 18, 2024), where a vishing victim who had never shared his OTP or card credentials was held not negligent, the bank's reliance on two-factor authentication notwithstanding, since the breach of authentication

safeguards through malware constituted a "deficiency in service" under Section 2(11) of the Consumer Protection Act, 2019. By contrast, in Suresh Chandra Singh Negi & Anr. v. Bank of Baroda & Ors. (Writ-C No. 24192 of 2022, Allahabad High Court), the Court declined relief where the petitioners had themselves generated the OTPs and approved the disputed transfers and had delayed reporting the incident, holding that the zero-liability circular operates as a shield for genuine victims and not as a sword for account-holders whose own conduct discloses negligence or concealment. These contrasting outcomes, together with the Bombay High Court's ruling in Jaiprakash Kulkarni & Ors. v. The Banking Ombudsman & Ors. (2024 SCC OnLine Bom 1666), illustrate that courts apply a fact-sensitive standard in which the burden of disproving negligence rests on the bank, but is displaced where the account holder's own conduct is shown to be reckless.

Two further judicial pronouncements have shaped the broader legal architecture within which digital banking fraud is investigated and prosecuted. In Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, a nine-judge Constitution Bench of the Supreme Court held that the right to privacy, including informational privacy over personal and financial data, is a fundamental right protected under Article 21 of the Constitution. This ruling directly catalyzed the subsequent enactment of the Digital Personal Data Protection Act, 2023, discussed in the following subsection, and continues to inform judicial scrutiny of how banks and payment intermediaries collect, store, and share customer data. Separately, in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1, the Supreme Court held that a certificate under Section 65B(4) of the Indian Evidence Act, 1872 (now Section 63 of the Bharatiya Sakshya Adhiniyam, 2023) is a mandatory precondition for the admissibility of electronic records, a requirement that has significant practical consequences for the prosecution of digital banking fraud, where bank server logs, transaction records, and call data records constitute the principal evidentiary basis for establishing the offence. Finally, the Supreme Court's decision in Shreya Singhal v. Union of India (2015) 5 SCC 1, which struck down the erstwhile Section 66A of the Information Technology Act as unconstitutionally vague and violative of free speech, remains a guiding precedent on the limits of cyber-legislation, and is frequently cited to caution against overbroad or imprecisely drafted cyber-financial offences. Most recently, in its suo motu proceedings on "digital arrest" scams (order dated February 9, 2026), the Supreme Court directed the Reserve Bank of India, the Ministry of Home Affairs, and the Department of Telecommunications to frame a uniform Standard Operating Procedure for the freezing and restoration of defrauded funds, observing that large-scale digital banking fraud amounts to "robbery and dacoity" and that banks cannot allow their digital infrastructure to function as a conduit for the seamless transmission of criminal proceeds.

3.2 The Digital Personal Data Protection Act, 2023: A Complementary Data Privacy Framework

Given that digital banking frauds such as phishing, identity theft, and SIM-swapping are fundamentally enabled by the unauthorized acquisition or disclosure of customers' personal and financial data, the Digital Personal Data Protection Act, 2023 (DPDP Act) constitutes an essential, if still maturing, addition to India's cyber-financial legal architecture. Enacted in August 2023 and brought into operative effect in a phased manner following the notification of the Digital Personal Data Protection Rules, 2025 on November 13, 2025, the DPDP Act is India's first comprehensive standalone data protection legislation, replacing the limited "sensitive personal data" framework that previously existed under Section 43A of the Information Technology Act, 2000 and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Banks and payment intermediaries, as "Data Fiduciaries" under the Act, owe a comprehensive set of obligations under Section 8: they must implement

reasonable security safeguards to prevent personal data breaches (Section 8(5)), notify both the Data Protection Board of India and every affected customer without delay in the event of a breach (Section 8(6)), establish an effective grievance redressal mechanism (Section 8(10)), and erase customer data once it is no longer necessary for the specified purpose, subject to statutory retention obligations such as the requirement under banking law to preserve KYC records for ten years after account closure. Under the Digital Personal Data Protection Rules, 2025, "reasonable security safeguards" are given concrete content, including encryption or tokenisation of personal data, access controls, and the maintenance of logs to enable detection and investigation of unauthorized access—measures directly relevant to preventing the data breaches that frequently precede digital banking fraud.

The DPDP Act is significant for digital banking fraud victims in at least three respects. First, its breach-notification regime under Section 8(6), operationalized through Rule 7 of the 2025 Rules, requires a Data Fiduciary to inform the Data Protection Board without delay and to furnish a detailed report within seventy-two hours, giving victims and regulators an early-warning mechanism that was largely absent under the IT Act regime. Second, Section 33 of the Act and the accompanying Schedule create a substantial deterrent through monetary penalties, with non-compliance with the security-safeguard obligation under Section 8(5) attracting penalties of up to Rs. 250 crore and failure to notify a breach under Section 8(6) attracting penalties of up to Rs. 200 crore, thereby incentivizing banks and fintech intermediaries to invest in stronger data security infrastructure. Third, Section 8(1) of the Act clarifies that a Data Fiduciary remains responsible for compliance "irrespective of any agreement to the contrary," preventing banks from contracting out of their data-protection obligations to third-party payment aggregators, business correspondents, or fintech partners through whom much digital banking fraud is perpetrated. At the same time, the DPDP Act does not create new criminal offences or compensation rights for individual data principals harmed by a breach; its penalty framework operates exclusively through the regulatory mechanism of the Data Protection Board, leaving the IT Act (Sections 43, 66, and 66C) and the BNS (Sections 316, 318, and 319) as the primary vehicles through which individual victims of data-enabled banking fraud obtain criminal redress. Effective protection against digital banking fraud therefore depends on the coordinated operation of the DPDP Act, the IT Act, the BNS, and RBI's sector-specific cybersecurity directions, rather than on any single statute in isolation (Hogan Lovells, 2025; Future of Privacy Forum, 2024).

4. Comparative Analysis: Rajasthan and Other States

A comparative assessment of cyber-financial crime across Indian states reveals significant disparities in incidence, institutional response, and policy innovation. According to the National Crime Records Bureau's Crime in India 2024 report, cybercrime crossed the one-lakh mark nationally for the first time, reaching 1,01,928 registered cases, a 17.9 per cent increase over 2023, with fraud accounting for the overwhelming majority of these offences. Telangana, Karnataka, and Maharashtra consistently report the highest absolute volumes of cybercrime among Indian states, a pattern attributable less to a higher underlying rate of victimization than to their large metropolitan digital economies, higher digital-payment penetration, and, in Telangana's case, a stated police practice of converting nearly every cyber complaint into a registered FIR. Rajasthan, by contrast, does not rank among the highest-volume states in absolute NCRB cybercrime statistics, but the state has experienced a steep proportionate rise, with cyber fraud complaints increasing from approximately 80,000 in 2023 to around 1.25 lakh by 2025, an increase of

roughly 25,000 cases annually. Table 1 below summarizes the comparative position of Rajasthan and four other major states.

Table 1: Comparative Overview of Digital Banking/Cyber Fraud Response – Rajasthan and Select States

State	Cybercrime/Cyber Fraud Volume (NCRB/NCRP data, approx.)	Key State Initiative	Comparative Observation
Rajasthan	~80,000 (2023) rising to ~1.25 lakh (2025); not among top NCRB-ranked states by absolute volume, but among the fastest-growing	R4C (Rajasthan Cyber Crime Coordination Centre, ₹100 crore outlay, 275 personnel); "Operation Cyber Shield"; police-station-level Cyber Help Desks and WhatsApp helplines	Rajasthan is positioning itself as the first state to replicate the central I4C model at state level, prioritizing speed of FIR registration and fund-freezing over the Telangana model of high registration volume
Telangana	27,230 cases (2024), highest in India, nearly 50% rise over 2023; highest cybercrime rate (over 70 per lakh population)	Dedicated Cyber Crime Police Academy unit; an estimated ₹20–25 crore invested in technology and officer training for victim-fund recovery	Officials attribute the high count partly to a policy of converting nearly every complaint into an FIR, suggesting that high registration reflects institutional responsiveness as much as underlying crime rate
Karnataka	21,003–21,889 cases (2023–24), second highest absolute volume nationally	Bengaluru-based Cyber Economic and Narcotics Crime (CEN) police stations in every district; specialized cybercrime cells with forensic labs	High volume concentrated in Bengaluru's IT corridor, illustrating that metropolitan digital-economy concentration, not state-wide diffusion, drives the numbers
Maharashtra	Highest volume of cybercrime complaints on the National Cyber Crime Reporting Portal nationally, around 3.03 lakh (2024)	Mumbai Police Cyber Crime Cell; state-wide cyber laboratories under the Maharashtra Cyber initiative	NCRP complaint volume far exceeds NCRB-registered FIRs, underscoring the gap between reporting and formal registration that

			affects most states except Telangana
Uttar Pradesh	10,794 cases (2023); third highest by NCRB count, second highest by NCRP complaint volume (~3.01 lakh, 2024)	UP Police Cyber Crime Cells at the district level; large population base drives high absolute numbers	Demonstrates that population size, rather than digital-economy concentration alone, can also drive high absolute cybercrime counts

Sources: National Crime Records Bureau, Crime in India 2023 and 2024 reports; National Cyber Crime Reporting Portal data as reported in IndiaSpend (2025); The420.in (2026); ETV Bharat (2025); BOOM Live (2025).

The comparison yields three principal insights. First, raw NCRB rankings can be misleading as a measure of either fraud incidence or institutional effectiveness, since Telangana's top position is partly an artefact of a deliberate policy of converting nearly all complaints into FIRs, whereas other states, including Rajasthan, register a far smaller proportion of reported incidents as formal cases. Second, the dominant national pattern is one of fraud concentrated in metropolitan, digitally-advanced commercial hubs (Bengaluru, Hyderabad, Mumbai), whereas Rajasthan's cybercrime growth, though numerically smaller in absolute terms, has been proportionately steep and increasingly extends into tier-2 towns and rural areas with comparatively lower digital literacy, posing a distinct enforcement challenge. Third, in terms of institutional innovation, Rajasthan's proposed Rajasthan Cyber Crime Coordination Centre (R4C) represents a notable governance experiment: by embedding bank nodal officers and technical experts within a state-level structure modelled on the central Indian Cyber Crime Coordination Centre (I4C), and by routing complaints directly to police stations rather than through the multi-tier I4C-to-district pipeline, Rajasthan aims to compress the time between fraud reporting and fund-freezing, an interval that critically determines whether defrauded money can be recovered before being layered through multiple mule accounts. Whether this model improves on the higher-volume but more metropolitan-centric approaches of Telangana, Karnataka, and Maharashtra remains to be empirically tested, but it illustrates that smaller and demographically diverse states such as Rajasthan can serve as policy laboratories for decentralized, victim-responsive cybercrime governance, provided such initiatives are matched with sustained investment in rural digital literacy and last-mile banking correspondent training.

5. Challenges in Prevention and Enforcement

The prevention and enforcement of digital banking fraud laws in India face numerous jurisdictional and evidentiary challenges that complicate effective legal action against offenders. Unlike conventional crimes, digital banking frauds frequently involve multiple actors operating across different geographical locations, often making it difficult to determine the appropriate jurisdiction for investigation and prosecution. Cybercriminals may execute fraudulent transactions from one state while targeting victims residing in another state or even another country. Such complexities create procedural hurdles for law enforcement agencies and judicial authorities. Additionally, electronic evidence presents unique challenges relating to authenticity, admissibility, preservation, and chain of custody, particularly in light of the Supreme Court's insistence in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1 that a Section 65B(4) certificate is mandatory for the admissibility of bank server logs, transaction

records, and other electronic evidence, a requirement that smaller police stations often struggle to satisfy promptly. Investigators must establish the integrity of digital records while ensuring compliance with legal standards governing electronic evidence. The dynamic and volatile nature of digital data increases the risk of evidence being altered, deleted, or concealed before authorities can secure it. Courts often rely on specialized forensic expertise to evaluate technical evidence, which may prolong legal proceedings and increase litigation costs. The absence of uniform procedures and varying levels of technological capacity among investigative agencies further complicate enforcement efforts. Consequently, jurisdictional and evidentiary issues continue to hinder the effective prosecution of digital banking frauds and underscore the need for procedural modernization and institutional capacity building (Brenner, 2022; Government of India, 2000/2008).

Cross-border cybercrime represents another significant challenge in combating digital banking fraud. Cybercriminals increasingly exploit the borderless nature of digital networks to conduct fraudulent activities from foreign jurisdictions while targeting Indian consumers and financial institutions. The use of virtual private networks (VPNs), encrypted communication platforms, cryptocurrency transactions, and anonymizing technologies enables offenders to conceal their identities and locations. As a result, identifying perpetrators and obtaining evidence often require international cooperation among law enforcement agencies, financial regulators, and judicial authorities. Mutual legal assistance treaties (MLATs), extradition arrangements, and international cybercrime conventions play important roles in facilitating cross-border investigations; however, differences in legal systems and procedural requirements frequently delay enforcement actions. Furthermore, many cybercriminal groups operate through decentralized networks that span multiple countries, making traditional investigative approaches less effective. The transnational character of digital banking fraud also raises questions regarding jurisdiction, applicable law, and enforcement authority. Without stronger international cooperation and harmonized legal frameworks, cybercriminals may continue to exploit regulatory gaps across jurisdictions. Therefore, addressing cross-border cybercrime requires coordinated global efforts, enhanced information sharing, and greater collaboration among national cybersecurity agencies (United Nations Office on Drugs and Crime [UNODC], 2023; INTERPOL, 2024).

A major obstacle in preventing digital banking frauds is the lack of digital literacy and consumer awareness among significant segments of the population. Although digital banking adoption has expanded rapidly, many users remain unfamiliar with cybersecurity risks and safe online practices. Fraudsters frequently exploit this knowledge gap through social engineering tactics, phishing emails, fraudulent calls, fake websites, and deceptive mobile applications. Elderly individuals, first-time digital banking users, and residents of rural areas are often particularly vulnerable to such schemes. In many instances, victims unknowingly disclose sensitive information, including passwords, OTPs, and banking credentials, thereby facilitating unauthorized transactions. Consumer awareness campaigns have been introduced by financial institutions and regulatory authorities; however, their reach and effectiveness remain inconsistent across regions. The rapid evolution of cybercrime techniques further complicates awareness efforts, as users must continuously adapt to emerging threats. Digital literacy is therefore not merely a technological issue but also a critical component of consumer protection and financial security. Strengthening public education initiatives and promoting cybersecurity awareness can significantly reduce opportunities for fraud and enhance resilience against digital threats (Organisation for Economic Co-operation and Development [OECD], 2023; Reserve Bank of India [RBI], 2024).

Institutional and technological limitations further impede efforts to prevent and combat digital banking

fraud. Many law enforcement agencies continue to face shortages of trained personnel, specialized cybercrime investigators, and advanced digital forensic resources. The increasing sophistication of cybercriminal methods often exceeds the technical capabilities available to local enforcement authorities. Similarly, financial institutions vary considerably in their cybersecurity preparedness and incident response capabilities. Smaller banks and financial service providers may struggle to invest in advanced security technologies due to financial and operational constraints. Technological challenges also arise from the rapid pace of innovation within the digital financial ecosystem. Emerging technologies such as artificial intelligence, blockchain applications, and decentralized financial platforms create both opportunities and new vulnerabilities. Regulatory agencies must continuously update their oversight mechanisms to keep pace with these developments. Furthermore, fragmented institutional coordination among regulators, law enforcement agencies, telecommunication providers, and financial institutions can delay responses to cyber incidents. Addressing these institutional and technological limitations requires sustained investment in capacity building, cybersecurity infrastructure, and inter-agency collaboration. Strengthening institutional resilience is essential for maintaining trust in digital banking systems and ensuring effective fraud prevention (International Monetary Fund [IMF], 2023; World Economic Forum, 2023).

Issues relating to victim compensation and grievance redressal constitute another significant challenge within the existing framework for addressing digital banking frauds. Victims often experience substantial financial losses and emotional distress following unauthorized transactions. Although regulatory guidelines provide mechanisms for reporting fraud and seeking reimbursement under certain circumstances, practical implementation remains inconsistent. Many consumers encounter difficulties in navigating complex complaint procedures, understanding eligibility requirements, and obtaining timely resolution of disputes. Delays in reporting fraudulent transactions may reduce the likelihood of fund recovery, particularly when funds are rapidly transferred through multiple accounts. Additionally, determining liability between consumers and financial institutions can be contentious, especially in cases involving allegations of negligence or compromised credentials. Consumer forums, banking ombudsman schemes, and grievance redressal mechanisms provide important avenues for relief; however, awareness of these remedies remains limited among many users. Effective compensation systems are essential for preserving consumer confidence in digital financial services. Therefore, strengthening grievance redressal mechanisms and ensuring transparent compensation procedures should remain central priorities within the broader strategy to combat digital banking fraud (Consumer Protection Act, 2019; RBI, 2024).

The cumulative effect of jurisdictional complexities, transnational cybercrime, digital illiteracy, institutional constraints, and inadequate redressal mechanisms highlights the multifaceted nature of challenges confronting digital banking fraud prevention. These obstacles demonstrate that technological solutions alone cannot effectively address cyber-financial crimes. A comprehensive response must integrate legal reforms, institutional strengthening, technological innovation, and consumer empowerment. Policymakers must recognize that cybercrime prevention requires continuous adaptation to evolving threats and changing technological environments. Collaborative efforts involving government agencies, financial institutions, technology providers, educational institutions, and civil society organizations are essential for developing sustainable prevention strategies. Furthermore, comparative analysis of successful practices adopted by different states and jurisdictions can provide valuable insights for improving enforcement effectiveness. By addressing existing challenges through coordinated and evidence-based approaches, India can strengthen its capacity to protect consumers, safeguard financial

systems, and promote trust in digital banking services. Ultimately, overcoming these challenges is crucial for ensuring the long-term success and security of the country's digital economy (World Bank, 2023; UNODC, 2023).

6. Conclusion and Recommendations

The present study demonstrates that digital banking has fundamentally transformed India's financial landscape by improving accessibility, efficiency, and financial inclusion. Technological innovations such as UPI, internet banking, mobile banking applications, and electronic payment systems have significantly enhanced consumer convenience and contributed to economic modernization. However, the rapid growth of digital banking has also created opportunities for cybercriminals to exploit technological vulnerabilities and human weaknesses. The analysis reveals that phishing, vishing, SIM-swap fraud, identity theft, malware attacks, and UPI-related scams have emerged as major threats to consumers and financial institutions. Existing legal mechanisms, including specific provisions of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, RBI guidelines, and consumer protection laws, provide an important regulatory foundation for addressing these challenges, a foundation that recent judicial pronouncements such as State Bank of India v. Pallabh Bhowmick have continued to refine. The comparative analysis further reveals that Rajasthan, while not among the highest-volume states by raw NCRB cybercrime count, has experienced a disproportionately steep rise in digital banking fraud and is responding through institutional innovations such as the proposed R4C, an approach that merits sustained empirical evaluation alongside the higher-volume but more metropolitan-centric responses of Telangana, Karnataka, and Maharashtra. Nevertheless, persistent issues relating to enforcement, jurisdiction, evidence collection, and consumer awareness continue to affect the effectiveness of anti-fraud measures. The findings underscore the need for continuous legal and institutional adaptation in response to evolving cyber threats. Therefore, digital banking fraud must be addressed through a holistic framework that integrates legal, technological, and educational strategies (Reserve Bank of India [RBI], 2024; World Bank, 2023).

One of the key conclusions emerging from this study is the necessity for a more uniform and comprehensive cyber-financial legislative framework. While various statutes and regulatory instruments currently govern different aspects of digital banking fraud, the legal landscape remains fragmented in certain respects. Overlapping provisions, procedural inconsistencies, and evolving technological realities can create uncertainty regarding enforcement and liability. A specialized legislative framework dedicated to cyber-financial crimes could enhance clarity, improve coordination among agencies, and strengthen consumer protection mechanisms. Such legislation should address issues relating to digital identity theft, electronic evidence, cross-border investigations, data protection, and victim compensation. Furthermore, harmonization between central and state-level enforcement mechanisms would promote consistency in the investigation and prosecution of digital banking offences. Comparative legal analysis indicates that jurisdictions with integrated cybercrime legislation often demonstrate greater effectiveness in addressing emerging threats. Consequently, legislative reform should remain a priority for policymakers seeking to strengthen India's cybersecurity governance framework and ensure the long-term integrity of digital financial systems (Kshetri, 2023; OECD, 2023).

Strengthening cyber policing infrastructure is another critical recommendation arising from this research. Effective prevention and enforcement depend heavily on the capacity of law enforcement agencies to investigate increasingly sophisticated cybercrimes. Specialized cybercrime units, digital forensic

laboratories, and trained investigators are essential components of a modern enforcement framework. Investments in advanced forensic technologies and analytical tools can significantly enhance investigative capabilities and improve the collection of admissible electronic evidence. Furthermore, law enforcement personnel should receive continuous training to remain updated on evolving cybercrime techniques and technological developments. Enhanced coordination among state cybercrime cells, financial regulators, telecommunication providers, and national cybersecurity agencies can further strengthen enforcement effectiveness. Comparative experiences from technologically advanced jurisdictions suggest that dedicated cybercrime infrastructure contributes significantly to higher detection rates and improved prosecution outcomes. Therefore, expanding institutional capacity and investing in specialized resources should constitute a central element of India's strategy for combating digital banking frauds (INTERPOL, 2024; Ministry of Home Affairs, 2024).

Consumer awareness and digital literacy must also be prioritized as essential preventive measures against digital banking fraud. Many cyber-financial crimes succeed because users lack adequate knowledge regarding online security practices and fraud prevention techniques. Educational initiatives should therefore focus on promoting awareness about phishing schemes, fraudulent communications, password security, safe digital payment practices, and reporting mechanisms. Public awareness campaigns should be tailored to different demographic groups, including senior citizens, rural populations, students, and first-time digital banking users. Financial institutions, educational institutions, government agencies, and civil society organizations should collaborate to develop comprehensive digital literacy programs. Integrating cybersecurity education into school and university curricula may also contribute to long-term improvements in consumer awareness. Given the dynamic nature of cyber threats, awareness initiatives should be continuous rather than episodic. Empowering consumers with knowledge and practical skills can significantly reduce opportunities for fraud and enhance the overall resilience of the digital financial ecosystem (International Telecommunication Union [ITU], 2023; RBI, 2024).

The study further recommends the strengthening of institutional mechanisms relating to victim compensation and grievance redressal. Timely reporting and efficient resolution of complaints are critical for minimizing financial losses and restoring consumer confidence. Existing mechanisms such as the Cyber Crime Helpline, National Cyber Crime Reporting Portal, Banking Ombudsman framework, and consumer dispute resolution forums should be further streamlined and made more accessible. Standardized procedures for handling digital banking fraud complaints can improve consistency and transparency in decision-making. Financial institutions should establish dedicated support systems capable of responding rapidly to reported incidents and coordinating recovery efforts. Additionally, regulatory authorities should periodically review compensation policies to ensure that consumers receive fair and timely relief. Effective grievance redressal not only benefits individual victims but also strengthens public trust in digital banking services. Therefore, improving compensation frameworks and dispute resolution mechanisms should remain a key objective of future policy reforms (Consumer Protection Act, 2019; Ministry of Home Affairs, 2024).

In conclusion, digital banking fraud represents one of the most significant challenges confronting India's rapidly expanding digital economy. While technological innovation has generated substantial benefits, it has simultaneously introduced complex legal, regulatory, and cybersecurity concerns. Addressing these challenges requires a coordinated strategy that combines legislative modernization, institutional strengthening, technological innovation, international cooperation, and consumer empowerment. Policymakers must adopt a proactive approach capable of anticipating emerging cyber threats and adapting

regulatory frameworks accordingly. Financial institutions must continue investing in cybersecurity infrastructure and consumer education, while law enforcement agencies require enhanced resources and specialized expertise. Ultimately, the effectiveness of digital banking fraud prevention depends upon the collective efforts of governments, regulators, financial institutions, technology providers, and consumers. By implementing the recommendations identified in this study, India can strengthen the security of its digital financial ecosystem and promote a safer, more resilient, and more trustworthy environment for digital banking transactions (IMF, 2023; UNODC, 2023).

References

1. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
2. Bhasin, M. L. (2022). Cyber frauds in digital banking: Emerging challenges and preventive strategies. Journal of Financial Crime, 29(3), 845–860.
3. BOOM Live. (2025). NCRB data on cyber crimes dated, not indicative of true picture: Experts. BOOM Live.
4. Brenner, S. W. (2022). Cybercrime and the law: Challenges, issues, and outcomes. Routledge.
5. CERT-In. (2024). Cyber security incident response and advisory framework. Ministry of Electronics and Information Technology.
6. Consumer Protection Act, 2019, No. 35 of 2019, India.
7. Digital Personal Data Protection Act, 2023, No. 22 of 2023, India.
8. ETV Bharat. (2025). Rajasthan Police launches ‘Operation Cyber Shield’ to tackle rising cyber crimes. ETV Bharat.
9. Future of Privacy Forum. (2024). The Digital Personal Data Protection Act of India, explained. Future of Privacy Forum.
10. Government of India. (2000/2008). Information Technology Act, 2000 (as amended in 2008). Ministry of Law and Justice.
11. Government of India. (2000/2008). Information Technology Act, 2000 (as amended in 2008). Ministry of Law and Justice.
12. Government of India. (2023). Bharatiya Nyaya Sanhita, 2023. Ministry of Law and Justice.
13. Hare Ram Singh v. Reserve Bank of India, W.P.(C) 13497/2022 (Del. HC, decided Nov. 18, 2024) (India).
14. Hogan Lovells. (2025). India’s Digital Personal Data Protection Act 2023 brought into force. Hogan Lovells.
15. IndiaSpend. (2025). #DataViz: How India’s cyber crime incidence is rising. IndiaSpend.
16. International Monetary Fund. (2023). Digital financial services and financial inclusion in emerging economies. IMF Publications.
17. International Monetary Fund. (2023). Digital financial services and financial stability report. IMF Publications.
18. INTERPOL. (2024). Global cybercrime threat assessment report. INTERPOL.
19. Jaiprakash Kulkarni & Ors. v. The Banking Ombudsman & Ors., 2024 SCC OnLine Bom 1666 (India).
20. Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
21. Kshetri, N. (2023). Cybercrime and digital payment security in emerging economies. Telecommunications Policy, 47(4), 102–118.

22. Kumar, R., & Sharma, P. (2022). Cybercrime and digital banking frauds in India: Legal challenges and regulatory responses. Indian Journal of Law and Technology, 18(2), 45–67.
23. Ministry of Electronics and Information Technology. (2023). Annual report on cyber security and CERT-In activities. Government of India.
24. Ministry of Home Affairs. (2024). Indian Cyber Crime Coordination Centre (I4C) annual report 2023–24. Government of India.
25. Nair, V. (2023). Consumer protection in the era of digital banking: Legal perspectives from India. Indian Journal of Consumer Law, 15(1), 55–78.
26. National Crime Records Bureau. (2026). Crime in India 2024. Ministry of Home Affairs, Government of India.
27. National Crime Records Bureau. (2025). Crime in India 2023. Ministry of Home Affairs, Government of India.
28. National Payments Corporation of India. (2024). UPI annual product statistics report 2023–24. NPCI.
29. Organisation for Economic Co-operation and Development. (2023). Digital finance and consumer protection. OECD Publishing.
30. Reserve Bank of India. (2023). Master directions on digital payment security controls. RBI.
31. Reserve Bank of India. (2024). Report on trend and progress of banking in India 2023–24. RBI.
32. Sharma, A., & Gupta, R. (2022). Legal regulation of cyber financial crimes in India. Indian Journal of Cyber Law, 7(2), 88–107.
33. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
34. Singh, P. (2024). The Bharatiya Nyaya Sanhita and emerging cybercrime challenges. Journal of Indian Criminal Law, 12(1), 21–39.
35. State Bank of India v. Pallabh Bhowmick & Ors., SLP No. 30677 of 2024 (Supreme Court of India, decided Jan. 3, 2025).
36. Suresh Chandra Singh Negi & Anr. v. Bank of Baroda & Ors., Writ-C No. 24192 of 2022 (Allahabad High Court) (India).
37. The420.in. (2026). Rajasthan strengthens cyber fraud control with ₹100 crore initiative. The420.in.
38. United Nations Office on Drugs and Crime. (2023). Global study on cyber-enabled financial crime. United Nations.
39. World Bank. (2023). Digital development and financial inclusion report. World Bank.
40. World Economic Forum. (2023). Future of digital payments and cybersecurity. World Economic Forum.