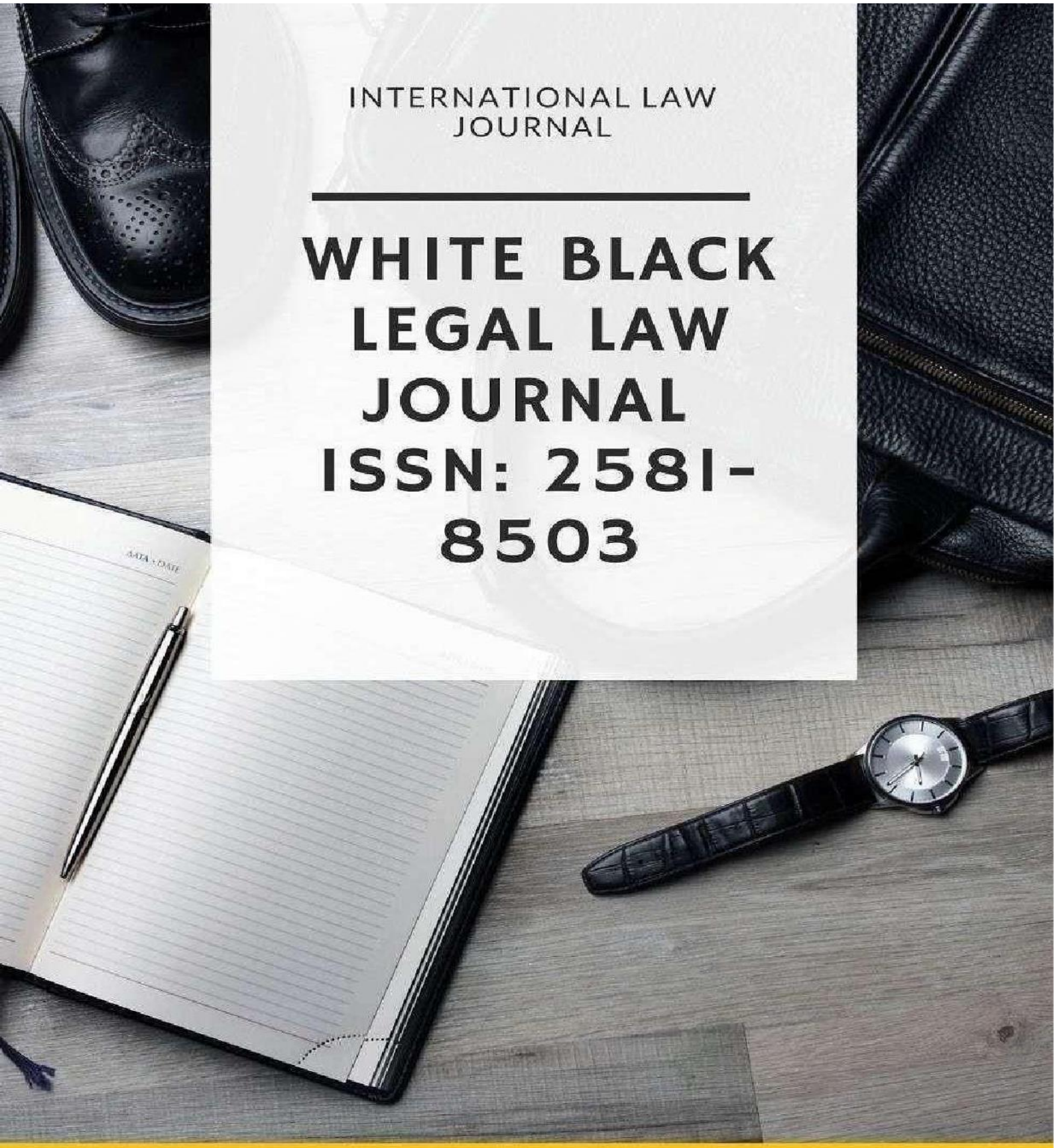

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 4 Issue 1 | Sep 2026 ISSN: 2581-8503

BANKING LAWS AND CYBERSECURITY IN INDIA: A CRITICAL STUDY OF LEGAL SAFEGUARDS AGAINST DIGITAL FINANCIAL FRAUDS

AUTHORED BY - HANEEF KHAN[1] & DR. GURJEET SINGH RATTA[2]

INTRODUCTION

The financial sector digitalization has made the way for banking and commerce in India altogether. The Indian economy has evolved from traditional banking systems to technologically driven financial ecosystems, with the advent of new technologies like internet banking, mobile banking, Unified Payments Interface (UPI), and digital wallets in the last 20 years. While this change has made financial systems more efficient and accessible, it has opened up new possibilities for financial fraud in the digital space. The incidence of cybercrimes like phishing, identity theft, SIM-swap fraud, ransomware attacks, and fraudulent loan recovery has been on the rise, which raises doubts about the effectiveness of the legal protection provided in India. In this context, this research critically analyses the existing legal protection against digital financial frauds in India, specifically the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (SARFAESI Act), Information Technology Act, 2000 (IT Act) and regulatory guidance and judicial precedents.

Empirical facts support the need for this inquiry. In the financial year 2024–25, Indian banks suffered a loss of ₹36,014 billion due to fraud, which is a 194% jump from the previous year, with digital-payment frauds accounting for 56% of the reported frauds.[3] Private banks reported the highest number of frauds with the main reasons being card and internet-banking related frauds, while public-sector banks suffered the most loss. These data only underscore the extent of the vulnerability in India's digital banking ecosystem and the pressing need to review the efficacy of legal protections.[4]

The SARFAESI Act, from a doctrinal point of view was enacted to enable banks and financial institutions to recover non-performing assets (NPAs) without the involvement of

[1] Research Scholar, Faculty of Law, Tantia University, Sri Ganganagar.
[2] Assistant Professor, Faculty of Law, Tantia University, Sri Ganganagar.
[3] Reserve Bank of India, Report on Banking Frauds 2024–25 (2025).
[4] Indian Computer Emergency Response Team (CERT-In), Annual Cybersecurity Report 2023 (2023).

courts.[5] It provided for the methods of recovery including securitisation, asset reconstruction and enforcement of security interests. As it has enhanced the rights of creditors, it has also been criticized for placing an excessive burden on borrowers and breach of due process and consumer protection issues, particularly in the digital era, where enforcement tools under SARFAESI like asset seizure and auction can easily be abused.[6] Consider the case of reports of recovery agents using digital platforms to harass borrowers, which are a danger to the misuse of such platforms, and judicial oversight has sought to balance these competing interests.[7] In Mardia Chemicals Ltd. v. Union of India, the Supreme Court upheld the constitutionality of the SARFAESI Act but invalidated the controversial provision that stipulated that 75% of outstanding dues would have to be paid before any appeal could be filed, stressing the need to put borrower safeguards in place.[8]

Simultaneously, the Indian IT Act, 2000, is the backbone of the Indian Cyber Law. While the IT Act has been praised for creating a legal framework for electronic records and digital signature, it has faced criticism for its narrow focus to deal with intricate financial frauds, and with a view to reforming the Act, the Jan Vishwas (Amendment of Provisions) Act, 2023 was passed.[9] Amended IT Act, 2008 added provisions pertaining to cyber terrorism, identity theft, and phishing, but these reforms were not sufficient to overcome the shortcomings of the Act. In addition, enforcement difficulties like inter-jurisdictional issues and less technical capability of law enforcement agencies further question the effectiveness of the IT Act in protecting the consumers from online financial frauds.[10]

Similar complexities emerge from judicial interpretations of the provisions of the IT Act. Unauthorised access to banking systems, fraudulent electronic transactions, and intermediary liability have been the subject of court cases. The judiciary has laid importance on consumer protection and due diligence by banks, but there is a lack of clarity in the legislation. Balancing banking regulation objectives and cybersecurity needs is difficult, especially when fraud is located on the intersection of banking and cyber.

Comparative perspectives further bring to light India's position. There are integrated frameworks to tackle digital financial frauds, such as in the United States, the United Kingdom and the European Union. Regulatory requirements for financial institutions are strict

[5] The Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, No. 54 of 2002, India Code (2002).
[6] R.K. Gupta, Banking Law and Practice in India 212 (3d ed. 2019).
[7] Press Trust of India, Digital Loan Recovery Frauds Rise in India, The Hindu (Jan. 12, 2023).
[8] Mardia Chemicals Ltd. v. Union of India, (2004) 4 SCC 311 (India).
[9] The Information Technology Act, No. 21 of 2000, India Code (2000).
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

across the UK, under the Financial Conduct Authority (FCA), and the European Union (EU) GDPR offers comprehensive data protection requirements; however, the Indian regulatory landscape is complex, consisting of banking laws, cyber provisions in the IT Act and regulatory guidelines, and may be lacking in coherence and integration. By comparing and contrasting, the best practices and lessons for India can be identified, especially in relation to harmonising banking and cyber regulations.[11]

Policy perspectives need to be considered. While the RBI has set guidelines for cybersecurity in banks,[12] there are some challenges in compliance, especially for smaller banks, and some area banks have conducted cybersecurity exercises, including a Cyber Security Exercise for the Banking Sector under India's G20 Presidency in 2023, which was organised by CERT-In.[13] Furthermore, new technologies like Artificial Intelligence, Blockchain, and Digital Forensics are also being developed that could be useful for fraud detection and prevention but are not widely used in India's financial sector.[14]

In the end, the strength of India's financial system hinges on the fortification of legal protections. Though the SARFAESI Act and IT Act are based, they need to be critically looked upon and may need to be amended to reflect the modern scenario. With the banking regulation being combined with cybersecurity needs, India can create a thorough framework that will give creditors the power they require, safeguard consumers, uphold due process, and foster trust in electronic financial transactions. The study, therefore, serves as a part of the current debate on law and technology and provides a glimpse into the issues and future of protecting the Indian financial system in the digital era.

REVIEW OF LITERATURE

The literature highlights the increasing concern for financial frauds in the banking system in the era of technology evolution at fast rates in India. The need for an adequate legal mechanism to address the challenges of frauds through the use of the internet has been a subject of deliberations by scholars, regulators and judicial machinery, among the most notable of which is the SARFAESI Act, 2002 and the Information Technology Act, 2000. This review is a critical synthesis of doctrinal, empirical and comparative studies to offer a critical overview of the state of scholarship. The evolution of digital banking has led to a rise in risks associated

[11] Financial Conduct Authority, Cybersecurity Standards for Financial Institutions (2022).
[12] Reserve Bank of India, Cybersecurity Framework for Banks (2016).
[13] CERT-In, Cyber Security Exercise for Banking Sector under G20 Presidency (2023).
[14] NITI Aayog, Blockchain: The India Strategy (2020).

with fraud. As digital banks evolve, so do the risk of fraud.

Digitalisation of Banking sector in India has been well documented. Their study indicates that the IT Act, 2000 has laid a legal foundation for electronic banking transactions, however, has the shortcomings in the enforcement systems to combat the advance frauds.[15] Likewise, Mishra and Singh point out that the transition from traditional to online banking has made identity theft and social engineering attacks more commonplace, calling for greater regulation.[16]

The SARFAESI Act and Banking Regulation.

The SARFAESI Act has received a lot of doctrinal study. In cases like Mardia Chemicals Ltd. v. Union of India that upheld the constitutionality of the Act but highlighted the need for borrower safeguards,[17] and other cases such as Nahar Industrial Enterprises Ltd. v. HSBC, where the judiciary confirmed that DRTs have jurisdiction over securitisation disputes, but civil courts have jurisdiction if fraud or forgery is involved, the court has tried to strike a balance between creditor rights and borrower protections.[18] The Supreme Court in Indian Overseas Bank v. Radhey Infra Solutions and Bank of India v. Sri Nangli Rice Mills Pvt. Ltd. restated the importance of procedural discipline under SARFAESI and the recognition of arbitration as a method of resolving inter-creditor disputes.[19]

In the era of digitalization, the unfairness of SARFAESI is compounded by the fraudulent recovery practices being carried out via online platforms, and this raises doubts as to its consumer protection and safeguards that are provided by the Act.[20] Patel also observes that the doctrinal perspective of SARFAESI is that its enforcement mechanisms are strengthened but the weakness of the SARFAESI Law is that it is not incorporated with cyber law and thus there are gaps in addressing frauds that are carried out using cyber technology.[21]

Cyber security and information technology act 2000.

The IT Act, 2000 has been severely criticized for its narrow definition of financial

[15] Seema Modi, Vanshika Premani & Mandeep Kaur, A Critical Analysis of E-Banking Frauds and Laws in India, Int'l J. Health Sci. 5(S2), 931 (2021).
[16] Sumit Mishra & Rajeev Kumar Singh, E-Banking Frauds in India: Critical Analysis, Int'l J. Res. & Analytical Reviews 12(3), 769 (2025).
[17] Mardia Chemicals Ltd. v. Union of India, (2004) 4 SCC 311 (India).
[18] Nahar Industrial Enterprises Ltd. v. Hong Kong & Shanghai Banking Corp., (2009) 8 SCC 646 (India).
[19] Indian Overseas Bank v. Radhey Infra Solutions, (2025 INSC 765); Bank of India v. Sri Nangli Rice Mills Pvt. Ltd., (2025 INSC 95).
[20] R.K. Gupta, Banking Law and Practice in India 212 (3d ed. 2019).
[21] Ajay Dayalji Patel, Emerging Trends and Legal Responses to Cyber Frauds in India: A Doctrinal Analysis, JETIR (2024

frauds. Jain and Shah's case study on how the IT Act (2000) helped mitigate cyber fraud in banking and Shah's doctrinal analysis of new cyber frauds have also shown that though the Act has been updated, it has been poorly enforced and has been unable to keep up with the new threat of cyber fraud.

An analysis of international comparisons shows that India is lacking in certain areas. The study suggests that the Indian regime needs to be unified, consumer-centric, and introduce more stringent liability regimes, with the reverse burden of proof, as seen in the UK, the US and the EU, and cyber insurance mechanisms. This reflects a general scholarly sentiment that the IT Act in India needs to be substantially altered to meet international practices.[22]

The regulatory guidelines and RBI framework.

The Reserve Bank of India has released multiple guidelines to enhance the cybersecurity in banks. The RBI's guideline for 2026 has put in place relief norms for consumers of small value digital frauds, restricting compensation to ₹25,000 and placing the burden of proof on banks.[23] This is a positive move towards consumer protection, but some contend the relief limit is not high enough.[24] CERT-In's Digital Threat Report 2024 for the BFSI sector revealed various new threats, including ransomware, insider manipulation, and frauds using AI, which further showed that cyber fraud has become a systemic risk and is being recognized by the government at an institutional level.[25]

Empirical Studies and Case Analyses.

Empirical studies give more insight. With the help of real life scenarios like Cosmos Bank cyberattack (2018), Mishra and Singh highlight that the vulnerability of Indian banks to malware-based attacks is compounded by a lack of digital literacy and delayed reporting of frauds. In the same manner, the Crime in India Report 2023 showed that a total of 86,420 cybercrime cases were reported in the country with almost 69% of the cases being financial in nature indicating the extent of victimisation.[26] This shows the need for preventive education and institutional capacity building.

[22] Sowmya B.M., Digital Banking Fraud and Regulatory Liability in India: Towards a Unified Consumer-Centric Legal Framework (2023).
[23] Reserve Bank of India, Digital Fraud Compensation Framework (2026).
[24] CERT-In, Digital Threat Report 2024 for BFSI Sector (2024).
[25] Press Information Bureau, CERT-In: India's Frontline Defender Against Cyber Threats (Jan. 23, 2026).
[26] NCRB, Crime in India Report 2023 (2023).

BANKING LAWS AND CYBERSECURITY IN INDIA – LEGAL SAFEGUARDS AGAINST DIGITAL FINANCIAL FRAUDS

India's digital banking landscape has seen swift growth, presenting systemic risks as well. India has emerged as one of the world's largest UPI digital payment markets, recording 45 billion transactions in 2023. However, along with these developments, various frauds have emerged like phishing, SIM swapping, ransomware and identity theft, which are regulated by two key legislations: Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (SARFAESI Act) and Information Technology Act, 2000 (IT Act) with RBI directives and sectoral regulations.[27]

SAFARSAESI ACT & FRAUD SAFEGUARDS

The SARFAESI Act was introduced to enable the banks and financial institutions to recover the non-performing assets even without the involvement of Courts.[28] It gives the power to the creditor to enforce security interest, to take over the assets, to auction the assets etc. In the digital era, borrowers have raised concerns on consumer protection due to the effective power of creditors in debt recovery at the cost of borrowers, including the use of the internet to fraudulently impersonate recovery agents.[29] These interests have been sought to be balanced by judicial review. The judiciary has been progressively taking on the responsibility of dealing with fraud risk within the ambit of SARFAESI in Mardia Chemicals Ltd. v. Union of India and more recently in Indian Overseas Bank v. Radhey Infra Solutions.[30]

IT Act, 2000 and Cybersecurity

Even though the IT Act has been reformed in the last couple of years, it still does not satisfy the requirements of the global standards such as EU GDPR Rules of 2019 that enforce strong data protection and notification rules in the event of a breach. Comparative scholarship suggests that India's framework is inadequate to tackle sophisticated frauds such as ‘Deep fake KYC Scams’ powered by AI.

[27] Anshuli Singh, Digital Banking and Cybersecurity Laws in India: Emerging Legal Challenges (2025).
[28] The Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, No. 54 of 2002, India Code (2002).
[29] R.K. Gupta, Banking Law and Practice in India 212 (3d ed. 2019).
[30] Mardia Chemicals Ltd. v. Union of India, (2004) 4 SCC 311 (India). And Indian Overseas Bank v. Radhey Infra Solutions, (2025 INSC 765).

Guidelines issued by the regulators and the framework by RBI.

The Reserve Bank of India (RBI) has issued several guidelines to enhance the cyber security of banks. Such measures highlight the institutional awareness of the risks associated with fraud, with CERT-In handling 15,92,917 cybersecurity incidents during 2023, and RBI's Digital Fraud Compensation Framework (2026) for providing relief of up to ₹25,000 for a small value fraud, with the onus of proof being shifted to banks.[31],14 However, there are compliance challenges, especially for smaller banks.

How judges are reacting to cyber fraud. Judicial reactions to cyber fraud.

The Indian judiciary has been increasingly tackling liability in digital fraud cases. The Allahabad High Court in Suresh Chandra Singh Negi v. Bank of Baroda has clarified that banks must refund unauthorized transactions if customers inform within three days of the occurrence of such transactions, as per RBI's circular.[32] In Jaiprakash Kulkarni v. Banking Ombudsman, the Bombay High Court frowned upon banks for their lack of implementation of the two-factor authentication (2FA) system, which led to the losses suffered by the customer.[33] These cases demonstrate the judiciary's emphasis on consumer protection and due diligence, while also showing the absence of adequate enforcement mechanisms.

Comparative Perspectives

Internationally, tighter liability systems have been introduced, for instance, in the UK and EU. The UK's Financial Conduct Authority has implemented regulations requiring an audit of cybersecurity for banks, while the EU's GDPR has stringent rules for data protection, which are not coherent in India where it exists in various parts of the SARFAESI, IT Act, RBI guidelines, and Consumer Protection Act. There is a call for a single framework that incorporates banking and cyber laws, full liability for unauthorised transactions and cyber insurance methods.[34]

[31] Reserve Bank of India, Digital Fraud Compensation Framework (2026).
[32] Suresh Chandra Singh Negi v. Bank of Baroda, Writ-C No. 24192 of 2022 (All. HC, July 17, 2025).
[33] Jaiprakash Kulkarni v. Banking Ombudsman, 2024 SCC OnLine Bom 1666.
[34] Ajay Dayalji Patel, Emerging Trends and Legal Responses to Cyber Frauds in India (2024).

CRITICAL ANALYSIS OF LEGAL SAFEGUARDS AGAINST DIGITAL FINANCIAL FRAUDS IN INDIA

The digitization of the Indian economy has grown at a significant pace with more than 45 billion UPI transactions in 2023. This is a sign of financial inclusion and efficiency; at the same time, it has brought to light systemic vulnerabilities. The top digital financial frauds include phishing attacks, SIM-swap frauds, ransomware, and identity theft. India's legal protection is enshrined in two key acts: the SARFAESI Act and the IT Act, which is complemented by guidelines issued by the RBI. However, their effectiveness is still questioned.

Strengths and weaknesses of SARFAESI Act.

• Strengths:

◦ Offers fast solutions for non-performing asset recovery to creditors.

◦ Shortens the civil litigation process.

• Weaknesses:

◦ Excessive rules on creditor rights are counterproductive to borrower protection.

There are still no effective regulations in place for fraudulent recovery activities on digital platforms.

Constitutional concerns are raised by judicial interventions (Mardia Chemicals Ltd. v. Union of India).

Enforcement provisions in the Act are effective but not tied to cyber law, resulting in a lack of synergy for tackling fraud enabled through digital technologies.

IT Act, 2000: Adequacy in the Digital Age

• Strengths:

◦ Relies on electronic records and transactions.◦ Creates legal recognition of electronic records and transactions.

◦ Contains provisions to criminalise identity theft and impersonation under Sections 66C–66D.

• Weaknesses:

◦ Restricted protection from advanced frauds including AI-generated deepfake KYC frauds.

◦ Ambiguities and lack of technical expertise in enforcement.

Comparative scholarship observes that India's existing data privacy laws are less

stringent than those of other jurisdictions such as the EU's GDPR, which sets out clear guidelines for data protection and notification of data breaches.

Guidelines and Regulatory Safeguards by RBI

To ensure the protection of consumers, RBI has introduced the norms of zero liability and digital lending guidelines (2022). Under its Digital Fraud Compensation Framework (2026), it set a cap of ₹25,000 on claims for small-dollar fraud cases, placing the responsibility to prove on the bank's side.

CERT-In also has a significant contribution with 15,92,917 cybersecurity incidents handled in 2023 and various threat reports published in their respective sectors for BFSI institutions. Compliance issues remain, especially in smaller banks that may not have the cyber security infrastructure to comply.

Judicial Responses

Consumer protection has been a theme of growing emphasis in Indian courts. The Allahabad High Court in the case of Suresh Chandra Singh Negi v Bank of Baroda decided to hold the banks responsible for unauthorised transactions, if customers reported the same in time. Likewise, in the case of Banking Ombudsman vs. Jaiprakash Kulkarni, the Bombay High Court had recorded its displeasure on the banks for not putting in place proper authentication system. These decisions highlight the courts' awareness of the vulnerability of consumers in digital fraud cases.

Comparative Perspectives

The United Kingdom: FCA requires that cybersecurity audits be carried out and places a strict liability on UUK for any unauthorised transactions.

EU GDPR includes comprehensive data protection and breach notification.

India: No coherence in the existing regulatory framework of SARFAESI, IT Act, RBI regulations and Consumer Protection Act.

There is a push for a single law combining banking and cyber law, that includes strict liability and cyber insurance.

Key Challenges

- Conditions for the transfer of the assets.
- Low capability of law enforcement.

- Lack of consumer knowledge of reporting mechanisms.
- Technological weaknesses, including deepfake KYC and ransomware.
- Compensation norms are inadequate, do not correspond to the size of losses.

CONCLUSION

A deep dive into legal protection against digital financial fraud in India uncovers an intricate and dynamic scenario where the existing banking legislation and the evolving regulatory framework for the digital economy don't always mesh entirely. The financial landscape has undergone a tremendous transformation with digital banking platforms, mobile apps, and electronic payment systems making financial transactions quicker, more accessible, and more inclusive. But, at the same time, this change has created a new set of risks to consumers, institutions, and even regulators. Phishing, identity theft, SIM-swap attacks, ransomware, and unauthorised digital lending are all forms of fraud that are becoming more prevalent, in part due to the lack of regulation in banks and cybersecurity in the digital world. From this study, it can be concluded that in India, the legislations like SARFAESI Act, 2002, IT Act, 2000, the regulatory guidelines issued by RBI and the surveillance by CERT-In are still scattered, reactive and lack proper integration to tackle the complexity of the modern financial frauds.

The main objective of the SARFAESI Act was to give power to banks and financial institutions to recover non performing assets, without the need for judicial intervention. It has enhanced the rights of creditors and facilitated debt recovery through its mechanisms of securitisation, asset reconstruction and enforcement of security interests. In the information age, however, the provisions of the Act are seen as having some serious drawbacks. Borrowers are vulnerable to harassment and exploitation when fraudulent recovery practices are undertaken using digital communication channels, online platforms, and through impersonation. While the Act is focused on empowering the creditors, this approach is essential for financial stability, may be counterproductive for consumer protection and due process. There have been some efforts in other jurisdictions to reconcile these interests, but SARFAESI does not have any specific provision to protect borrowers from digital fraud. In the absence of the reform to the Act, however, that would include cyber protections and consumer-centric safeguards, the Act has limited relevance in addressing digital financial frauds.

However, the Information Technology Act, 2000 (IT Act), was India's first attempt towards regulating electronic transactions and cybercrimes. Its provisions on electronic

records, digital signatures and offences like identity theft, impersonation etc, paved the way for cyber law in India. Changes in 2008 added cyber terrorism and phishing to its coverage, and subsequent changes attempted to modernize adjudication processes. However, the IT Act is still not as up-to-date as the sophisticated nature of the crimes being committed today. The Act is inadequate in the face of new risks, like AI-based deepfake KYC scams, ransomware attacks on banking systems, and massive data breaches. Enforcement issues such as jurisdictional issues, insufficient technical capacity on the side of enforcement bodies and consumer ignorance also hinder its effectiveness. In contrast to other international laws like the EU's GDPR, which requires all data to be protected and that any breaches be notified, the IT Act in India is very basic. This deficiency highlights the need for a comprehensive revision of cyber law to bring it in line with international standards, and to meet the challenges of digital financial fraud.

The gaps have been tried to be addressed in the regulatory guidelines laid down by the Reserve Bank of India and through surveillance by CERT-In. RBI's circulars on customer protection, liability in unauthorised transactions and guidelines for digital lending are some significant strides towards empowering consumers. Banks' adoption of compensation standards for small-value frauds puts the onus on the banks, which is a recognition of consumer vulnerability. CERT-In is playing a vital role in cyber monitoring, threat advisory and holding cyber security exercise in the various areas of the economy, which has helped build institutional capabilities. However, there are ongoing compliance issues, especially for smaller banks and financial institutions who are resource constrained. Furthermore, maximum compensation limits are still not high enough compared to the amount of damage inflicted upon the consumers. These regulation steps, although progressive, are reactionary and fragmented and will not provide sufficient cohesion and integration to create a comprehensive defense against digital financial frauds.

Judicial rulings have increasingly focused on consumer protection, when banks have been found liable for unauthorised transactions and lack of proper security measures. Courts have set standards for liability, faulted on deficient authentication processes, and emphasised the need for due diligence. These decisions mark an evolution in the understanding of consumers' vulnerability in digital fraud cases. But judicial rulings often show that the law is not always as clear as much as it needs to be, especially when it comes to balancing the goals of banking regulation with cybersecurity requirements. Although the judiciary has a vital role to play, they can by no means replace thoroughgoing legislative reform. In the absence of specific legislation on digital fraud, there are fewer judicial decisions and they have limited

scope and effect.

Comparative perspectives further highlight India's shortcomings. The UK and the EU have introduced a banking regulatory regime which incorporates cybersecurity requirements. The Financial Conduct Authority (FCA) in the UK has strict cybersecurity audits, and the GDPR in the EU offers comprehensive data protection measures. India's regulatory landscape is disjointed with SARFAESI, IT Act, RBI guidelines and consumer protection laws being uncoordinated and unintegrated. The scholars plead for securing a uniform system of banking and cyber laws, severe liability for any unauthorized transactions and integration of tools like cyber insurance. Such reforms would allow India to catch up with the world best practices and enhance India's resilience to digital financial frauds.

The issues that remain are complex. SARFAESI and the IT Act both have overlapping jurisdictions, causing confusion in enforcing the laws. Investigation and prosecution is a challenge due to weak institutional capacity of law enforcement agencies. Poor victimisation awareness among consumers makes it harder to deal with. As the technology behind these vulnerabilities continues to advance at a rapid pace, the legal countermeasures fall behind.The technologies behind these vulnerabilities grow more sophisticated than the legal countermeasures. The level of compensation is still not commensurate with consumer losses. These issues highlight the need for improvements in existing safeguards and their shortcomings.

The final answer that comes to mind is that while the legal framework for preventing digital financial frauds is solid, it is still inadequate, given the changing nature of the threats. SARFAESI Act empowers the Creditors but not the borrowers from the fraudulent practices in the digital world. The IT Act outlaws cyber fraud but is weak against the sophisticated scams. RBI guidelines and CERT-In interventions bring relief but compliance issues. Consumer protection is emphasised by judicial decisions and the lack of clarity in legislation. By comparing India's existing financial and cyber regulations, it becomes clear that a more comprehensive approach to banking and cyber law is necessary to address these challenges.The comparative analysis highlights the need for a more holistic approach to banking and cyber law in India, emphasising the integration of technological advancements like artificial intelligence in fraud detection and blockchain-based transaction security, alongside a need for more stringent liability frameworks.

Going forward India needs to take a multipronged approach. Legislative changes are needed to bring banking and cyber laws together in a single code, ensuring a healthy balance between creditors' and consumers' rights. Rather, there should be stricter liability norms and

comprehensive data protection and breach notification norms in the regulatory measures. Capacity needs to be enhanced at the institutional level through training, resources and inter-agency coordination. Consumer awareness campaigns need to be expanded to enable consumers to identify and report fraud. The use of technological solutions, such as artificial intelligence, blockchain and digital forensics, must be leveraged to detect and prevent fraud. International cooperation and compliance with international standards are needed to combat the cross-border frauds.

In conclusion, protecting India's digital financial ecosystem calls for a paradigm shift from fragmented and reactive to integrated and proactive strategies. A strong financial system relies on empowering lenders and also safeguarding consumers and maintaining fair and reliable processes, as well as building trust in electronic transactions. India can create a secure, inclusive and robust financial ecosystem by redefining its safeguards. This study therefore serves to conclude that there is still much to be done, although there has been great improvement. The future of India's digital economy depends on the adaptability, innovation and protection of its legal framework in the face of the changing threats of digital financial frauds.