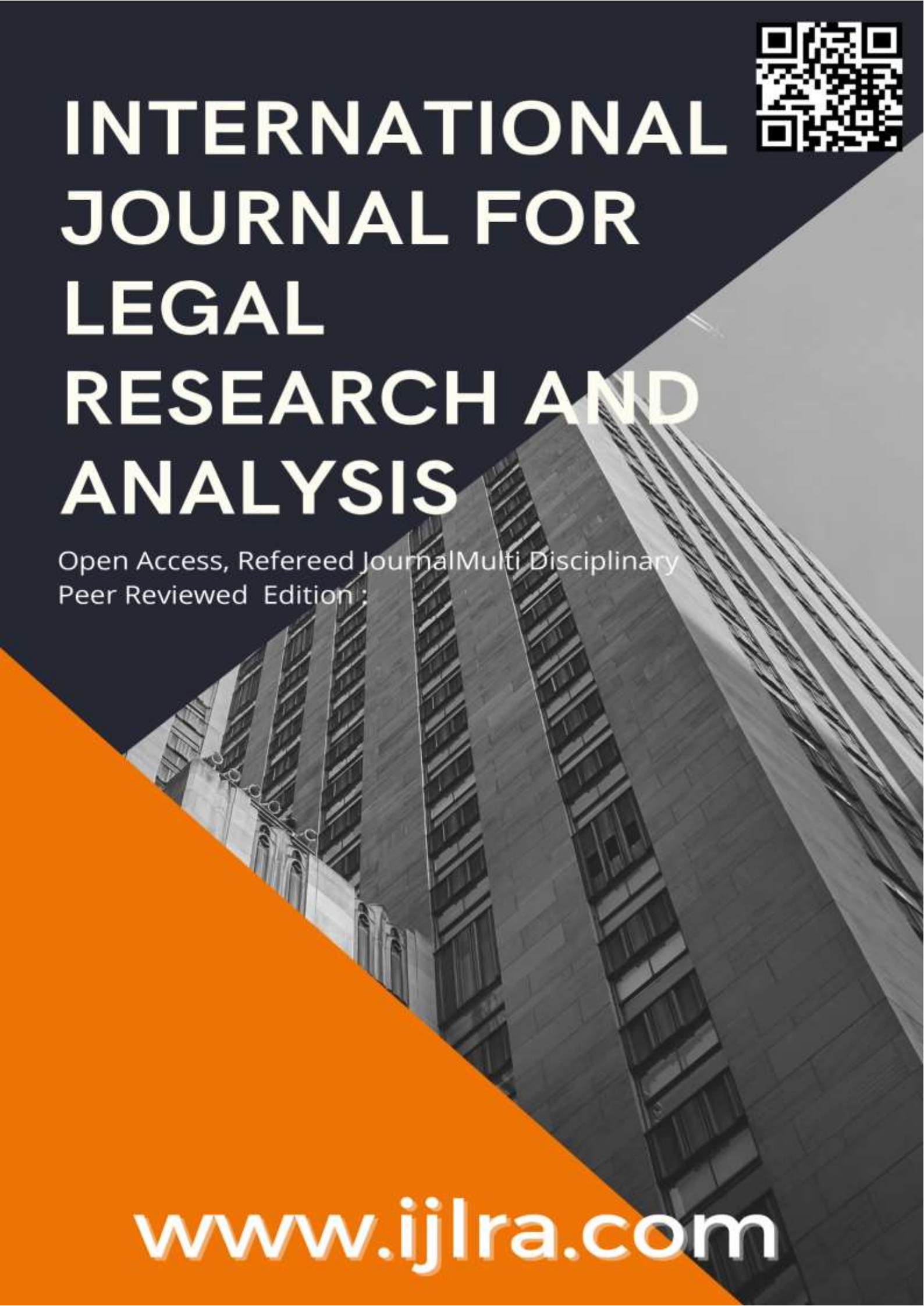
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :



www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

"BANKING LAWS AND DATA PROTECTION IN THE DIGITAL AGE: ENHANCING SECURITY OF ELECTRONIC FUND TRANSFERS IN INDIA"

AUTHORED BY: NANDANI RATHORE
(LLM National Law Institute University Bhopal)

Abstract

This study provides a comprehensive analysis of the regulatory and legal frameworks governing Electronic Fund Transfers (EFT) in India, emphasizing fraud protection. It begins with a historical overview of EFT and its various modes, highlighting the benefits and the necessity of two-factor authentication. The analysis then delves into the Digital Personal Data Protection Act, 2023 (DPDPA), examining its impact on EFT security through the establishment of a Data Protection Authority, protective provisions, and enforcement mechanisms. Further, it explores the intricate legal and regulatory frameworks, alongside the role of judicial activism in shaping and enforcing EFT regulations. Through a meticulous review of existing laws and recent judicial interventions, this study aims to propose actionable suggestions to enhance the security and efficiency of EFT systems in India. The findings underscore the need for robust data protection and regulatory oversight to mitigate fraud and enhance trust in digital financial transactions

Introduction

E-banking refers the practice of doing banking transactions through a personal computer via the internet. Bank Customers can conduct banking transactions online, including electronic funds transfers (EFT) between connected accounts, loan applications, and transactions such as enrolment repayment, bill payment, and so on. Electronic Funds Transfer is a method of moving money from one bank account to another without using banknotes or coins. It refers to computer-based systems that accomplish financial transactions electronically by exchanging or transferring money inside the same financial institution or across numerous institutions using a digital terminal, telephone, or computer.[1]

[1] Sonia Chawla and Ritu Singhal, 'India and the World: The Changing Paradigms in the Banking Sector due to Technological Advancements' Prajnan, (2010) 6 (3) Law Journals Organisation.

 ISSN: 2582-6433

EFT is a group of technology that enables the completion of financial transactions with electronic signals instead of paper money. Direct deposit is one of the most often used EFT methods, where payroll is deposited straight into an employee's bank account. Conversely, EFT encompasses all forms of electronic fund transfers, including those made using credit cards, Automated teller machines (ATM), Fed wire transfers, and point-of-sale (POS) systems.[2]

The mechanism facilitates computerized fund transfers between banks. Most EFT systems use computers, communication networks, and automated data files. ATMs are widely available for 24-hour deposits and withdrawals. EFT is expected to replace cash and cheques as the principal payment method for products and services, as well as other financial activities.[3]

The digital transaction eliminates the need for excessive documentation. Because of its simple steps, EFT has become the most popular method of transferring funds. It is also the most convenient and straightforward manner of payment. The increased use of EFT is leading to a decrease in the use of paper cheques.[4]

Sender and recipient of payments are the two parties that typically participate in an EFT transfer. When a transfer is started by the sender, an EFT payment procedure begins. The payment request originates from a payment terminal via the internet and travels through a number of digital networks. A request is sent to the recipient's bank by the sender's bank.

Senders might range from individuals to businesses. They might give money to a service provider, a vendor, or an employee. Similarly, beneficiaries might be organizations or people, such as workers, suppliers of goods, retailers, utility companies, and service providers.[5]

The foundation of an electronic money transfer system is the use of the internet to conduct virtual world transactions. What matters is that a formal record of the transactions is created, even though

[2] Satish Chandra, 'Electronic Funds Transfer: Exploring the Difficulties of Security' (2019) 5 (4) Journal of International Commercial Law and Technology <https://media.neliti.com/media/publications/28771-EN-electronic-fundstransfer-exploring-the-difficulties-of-security.pdf> accessed on 11 March 2024.
[3] Van Jaarsveld, 'Domestic and International Bank Supervision and Regulation-Defying the Challenges' (2020) 119 (3) South African Law Journal 71.
[4] Samir Mohammed Ali Abdulah, 'Legal Risk Associated with Electronic Funds Transfer' (2018) 17 (1) Plymouth Law School <https://pdfs.semanticscholar.org/3cd1/7d4de3b800a46aa07d55172c55096084058d.pdf> accessed on 11 March 2024.
[5] Mpakwana Annastacia Mthembu, 'Electronic Funds Transfer: Exploring the Difficulties of Security' (2018) 5(4) Journal of International Commercial Law and Technology, <https://media.neliti.com/media/publications/28771-ENelectronic-funds-transfer-exploring-the-difficulties-of security.pdf> accessed on 11 March 2024.

 ISSN: 2582-6433

they are carried out directly between the parties. An additional benefit of this is that it saves time compared to issuing various negotiable documents, cashing them, or going to the bank to conduct transactions. With a single finger tap, any electronic fund transfer transaction can be completed.[6]

LITERATURE REVIEW

Mohan Lal Tannan and Rajesh Narain Gupta in their book "ML Tannan Banking Law and Practice in India"[7] examines pertinent legal frameworks and legislation that can be used to improve EFT security, even though it is not exclusively focused on EFT. It explores the best practices and changing laws for protecting these kinds of transactions. The book provides readers with the skills to recognize vulnerabilities by analyzing contemporary threats such as fraud and data breaches. In order to protect compliance, it examines pertinent laws and Reserve Bank of India (RBI) recommendations. Through an analysis of recent modifications to The Information Technology Act, the book provides valuable perspectives on constructing a strong legal structure to safeguard EFTs. Banks, financial institutions, and consumers are better equipped to navigate the digital financial landscape with increased security and confidence and also the book provides insightful analysis of significant cases and legal precedents for interested parties seeking to establish a more reliable and safe electronic fund transfer environment in India.

Sankalp Jain in his paper "Electronic Fund Transfers: A Critical Study in Indian Context with Special Reference to Security & Privacy Issues"[8] Examine the significance of electronic fund transfers in India's banking industry. also provide a quick overview of EFT's origins. The forms of electronic payment systems and electronic banking methods in India are covered in the second chapter of his paper. The third and fourth chapters, which comprise the main body of this work, will focus on the legislative framework governing electronic funds transfers in India and the related challenges. The fifth and final chapter, which is the conclusion, will provide insight into the future roadmap for the electronic payment system. To put it another way, it will assess the system's efficacy and offer additional suggestions for enhancements, particularly with regard to security and privacy.

[6] M.L Tannan, Tannan's Banking Law and Practice in India (23rd edn 2010).
[7] Mohan Lal Tannan and Rajesh Narain Gupta, ML Tannan Banking Law and Practice in India (Lexis Nexis 2017).
[8] Sankalp Jain, 'Electronic Fund Transfers: A Critical Study in Indian Context with Special Reference to Security & Privacy Issues' (SSRN, 28 January 2018) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208110 > accessed on 12 March 2024.

 ISSN: 2582-6433

Rimpi Jatana in her book "E-Banking in India: Challenges and Opportunities"[9] examines the rapidly expanding field of electronic banking in India. It emphasizes the effectiveness and simplicity that E-banking provides across a variety of platforms, including the internet, mobile devices, and ATMs. The book doesn't downplay the difficulties that come with this advancement in technology, though. Cyberattacks and data breaches are examples of security dangers that are carefully considered, and strong regulatory frameworks are necessary to guarantee consumer protection. The Reserve Bank of India's current legislative rules are acknowledged in the book, but it also stresses the necessity of ongoing adaptation in order to stay up with rapidly advancing technologies. Book investigates how E-banking affects financial inclusion, especially for people who live in distant areas. Through a thorough analysis of these prospects and obstacles, the book provides insightful information to banks, policymakers, and consumers, clearing the path for an E-banking environment in India that is safer and more inclusive.

STATEMENT OF PROBLEM

There are serious security and privacy issues with India's electronic fund transfer system, which frequently results in fraudulent activity. Even with security precautions in place, there are always gaps that allow unwanted access to private financial data and transactions. The financial stability of the customers is jeopardized by these breaches. To protect the integrity of electronic fund transfers and rebuild trust in India's banking system, these issues must be resolved.

HYPOTHESIS

Implementing the Digital Personal Data Protection Act, along with strong security measures like multi-factor authentication and real-time transaction monitoring, will improve security and privacy in India's electronic fund transfer system, effectively reducing fraudulent activity and restoring trust in the banking sector.

RESEARCH OBJECTIVES

Following is the research objective of the study: -

1. To determine the efficiency of the Digital Personal Data Protection Act.
2. To investigate the effects of multi-factor authentication on security.
3. To study the relevant laws protecting EFT in India.
4. To recommend robust measures to enhance EFT security and privacy.

[9] Rimpi Jatana in her book, E-Banking in India: Challenges and Opportunities (New Centaury Publications 2007).

 ISSN: 2582-6433

RESEARCH QUESTIONS

Following are the research questions of the study: -

1. Whether the Digital Personal Data Protection Act, 2023 has greatly increased the effectiveness of privacy protection in EFT systems.
2. Whether adopting multi-factor authentication improved security in India's EFT system.
3. Whether real-time transaction monitoring is beneficial in preventing fraudulent electronic fund transfers.
4. Whether current restrictions are sufficient to prevent fraud in India's electronic fund transfer system.

RESEARCH METHODOLOGY

The research methodology for this study will be doctrinal, and it will examine pertinent statutes, case law, and regulatory guidelines related to electronic fund transfers in India. It will entail an in-depth review of the current legal systems and how effectively they handle problems relating to electronic fund transfers. The researcher will follow the OSCOLA (4th edition) citation style throughout the research.

SCOPE AND LIMITATION

This study evaluates the influence of legal and technological measures on the security and privacy of India's electronic fund transfer system, with the goal of identifying and recommending improvements. Limitations include the continually developing nature of cyber threats and the variety in security measures implemented by different banking organizations.

TENTATIVE CHAPTERISATION

1. Introduction
2. General Overview of Banking Laws and Regulations Protecting frauds in EFT in India.
3. Examining the Digital Personal Data Protection Act and How It Affects Electronic Fund Transfers.
4. Regulatory Framework and Judicial Activism in EFT in India.
5. Conclusion and Suggestions

 ISSN: 2582-6433

CHAPTER-2

General Overview of Banking Laws and Regulations Protecting frauds of EFT in India

(2.1) ORIGIN OF EFT: - The first ATM, which could handle account transfers, accept deposits, and provide quick cash withdrawals, was established in the 1960s, which is when EFT first emerged. EFT was a feature of the system that allowed transactions to be made without using either in cash or cheques. With the assistance of numerous proposals made by various Committees, RBI launched the push for electronic banking. Technology was being employed by banks in 1984 to enhance internal operations and communication amongst branch offices. As recommended by the Rangarajan Committee Reports in Computerization of Banks, the primary goal in 1994 was to introduce technology breakthroughs in the payment systems. The report supported the launch of the EFT system, the implementation of MICR clearing for over 100 banks, and the promotion of the "card culture" idea. The RBI then introduced EFT in 1995 with the goal of modernizing the nation's financial transfer system and accelerating bank-to-bank transactions.[10]

In addition, the Narsimha Committee Report (1998) concentrated on matters such as enhancing the financial system, modernizing technology, and developing human resources. The Committee emphasized the need for clarification on a number of concerns pertaining to EFT authentication. A different committee led by Dr. A. Vasudevan suggested even more technological advancements for the banking industry. These included computerizing government transactions, outsourcing technology and services, and creating a legal framework for electronic banking. Established in 1999, the Indian Financial Network (INFINET) functions as the central hub for communication within the Integrated Payment and Settlement System (IPSS). A "Working Group" on Internet Banking was established by the RBI to look into various Internet banking-related issues.[11]

The Indian government took these concerns into account and passed the Information Technology Act, 2000 to give electronic transactions legal recognition. In addition, an amendment to the RBI Act was made, granting the RBI the authority to control electronic transfers between financial institutions.

(2.2) MODES OF ELECTRONIC FUND TRANSFER

India provides a range of electronic funds transfers choices to accommodate varying requirements

[10] R. K. Mittal and Sanjay Dhingra, 'Technology in Banking Sector: Issues and Challenges' (2006) 27(14) Indian Journal of Banking Institution.
[11] Working Group on Internet Banking, 2001 under the Chairmanship of S.R. Mittal.

 ISSN: 2582-6433

and degrees of urgency. The four most typical types are as follows:

1. **National Electronic Fund Transfer (NEFT): -** Money transfers between bank accounts are frequently done via NEFT. Its simplicity of use has led to its widespread usage for salary payments. Funds, however, settle in batches and may require up to three business days (T+3). Even while there isn't a set limitation, some banks may have restrictions (SBI, for example, caps retail NEFTs at Rs. 10 lakhs). For NEFT transactions to other banks normally levy fees ranging from Rs. 2.50 to Rs. 25, contingent on the amount sent. NEFT can only be used on bank working days and transfers made on weekends or holidays are handled the next business day. Nowadays, NEFT service is available around-the-clock at certain institutions. The recipient's name, bank, account number, and IFSC code are required in order to start a NEFT transfer.[12]
2. **Real Time Gross Settlement (RTGS): -** RTGS is an electronic funds transfer method by which transactions are processed promptly on a gross basis, that is, individually rather than in batches. It enables for the instantaneous movement of funds between banks and financial organizations. RTGS ensures the secure and real-time settlement of high-value transactions, with no delays or waiting periods, hence increasing efficiency and lowering risk. It's widely utilized for high-value, time-sensitive transfers like interbank payments, stock trading, and significant corporate transactions. To ensure financial stability and integrity, RTGS systems are supervised by central banks or monetary authorities.[13]
3. **Immediate payment Service (IMPS): -** In India, IMPS is electronic payments transfer system that facilitates instantaneous interbank transactions around-the-clock, even on weekends and public holidays. It enables users to transfer money swiftly and safely using ATMs, internet banking, and mobile phones. The real-time operation of IMPS makes it possible for money to be transferred between bank accounts right away. It's extensively utilized for a number of things, including peer-to-peer transfers, commercial transactions, and bill payments. Because IMPS transactions are executed instantaneously, users can perform financial transactions anywhere, at any time, with ease and flexibility. The speed and effectiveness of electronic financial transfers in India's banking industry have been greatly increased by this technology.[14]

[12] Sahira Irfana, Aarti Raghurama, 'Innovation of Indian Banking: Extent of Precautions Taken by the Customers While E-Banking' (2013) 8 (5) IOSR Journal of Business and Management 1.
[13] Akram Jalal, 'Evaluating the Impacts of Online Banking Factors on Motivating the Process of E- banking' (2019) 1 (1) Journal of Management and Sustainability 34-37.
[14] Umamaheshwari Mahant., Savitri Sivasubramanian. & Harish Kumar, 'Online Credit Card Transaction Using Finger Print Recognition' (2010) 2(3) International Journal of Engineering and Technology 320- 322.

 ISSN: 2582-6433

4. **Unified Payment Interface (UPI): -** In India, UPI is a real-time, instantaneous payment system that facilitates easy money transfers between bank accounts through smartphones. With UPI, customers can connect several bank accounts into a single mobile app, making transactions simple and safe. People can use UPI to transfer money, pay bills, and make purchases straight from their bank accounts without using conventional banking information like account numbers or IFSC codes. It provides quick transaction resolution and is operational around-the-clock. By providing a practical, universal, and inclusive digital payment platform, UPI has transformed EFT and encouraged financial inclusion and innovation within India's payment ecosystem.[15]

(2.3) BENEFIT'S OF EFT

1. The beneficiary does not require the remitter to send a physical check or demand draft.
2. The beneficiary can deposit the paper instruments without having to go to his bank.
3. The beneficiary does not have to worry about tangible instruments being lost, stolen, or subject to fraudulent encashment.
4. An email or SMS confirming the remittances' credit.
5. The remitter may also use online banking to start remittances from his place of employment or residence.[16]

(2.4) TWO FACTOR AUTHENTICATION

Online accounts are made even more secure with two-factor authentication (2FA), especially when it comes to EFTs. 2FA necessitates a second verification step during login or transactions, in contrast to depending just on a password. This extra element could be a fingerprint scan, a temporary code delivered via SMS, or even an authentication app on your phone. Gaining unwanted access is made much more difficult by requiring both the password and this additional factor. To make EFTs and online accounts safer for all parties, 2FA functions as an additional security layer, similar to using both a key and a fingerprint scan to access your home.

[15]S.P Singh, Shukla, N. Rakesh &V. Tyagi, 'Problem Reduction in Online Payment System Using Hybrid Model' (2020) 3(2) International Journal of Managing Information Technology (IJMIT) 71.
[16] Ashish Verma, 'Phishing Attacks and perceptions of service quality: An Analysis of Virtual Banking in India' (2019) 3(1) AEIJST 13.

 ISSN: 2582-6433

CHAPTER-3

Examining the Digital Personal Data Protection Act and How It Affects Electronic Fund Transfers

(3.1) INTRODUCTION: - The adoption of the Digital Personal Data Protection Act, 2023 (DPDPA) has a substantial impact on EFT in India. This act intends to provide individuals control over the personal data utilized by financial institutions during EFTs. The DPDPA attempts to limit the risk of data leaks and unauthorized access by requiring rigorous data security mechanisms as well as user authorization for processing.[17] Furthermore, the act gives individuals the opportunity to seek modifications or deletion of personal data, promoting greater transparency and accountability throughout the EFT ecosystem. This strengthened data protection environment promotes trust and security to both individuals and financial institutions who conduct EFTs, thereby protecting sensitive financial information and preventing fraudulent activity.[18]

(3.2) ESTABLISHMENT OD DATA PROTECTION AUTHORITY

A specific Data Protection Authority (DPA) is established by the DPDPA and is in charge of:

1. **Creating norms and guidelines:** To ensure uniformity throughout the financial industry, the DPA will publish detailed guidelines on data security measures and user consent processes for electronic fund transfers.
2. **Examining data breaches:** The DPA has the authority to look into incidents and hold accountable the financial institution that may have caused the breach after being notified of one.
3. **Resolving consumer complaints:** If people feel that their data rights were abused throughout the EFT procedure, they can file a complaint with the DPA.[19]

(3.3) PROVISIONS OF DPDPA PROTECTING EFT

1. **Data Minimization:** DPDPA improves EFT data security through data reduction. This principle compels financial institutions to gather and maintain only the information that is strictly essential for EFT transactions. This decreases the quantity of sensitive financial data accessible in the event of a breach. Imagine your bank merely holding the recipient's

[17] Deepak Kumar and Shashi Kapoor, 'Internet Banking: A New Paradigm' (1st edn, New Century Publications 2019) 42.
[18] Tschentscher. A, 'Privacy and Data Protection by Rules Rather than Principles' (2022) 4 (1) SSRN Electronic Journal.
[19] Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2(1) Eur. Data Protection Law Review 28.

 ISSN: 2582-6433

account information for an EFT, rather than your whole financial history "less data, less danger" This technique lowers the possible impact of data breaches and increases trust in the Indian EFT ecosystem.[20]

2. **User Consent:** When using DPDPA with user consent, user have control over EFTs. The bank needs users' express consent to gather, use, and disclose the personal information related to the EFT before it can begin. This openness adds a degree of protection and gives the power to see how users' data is utilized. Encouraging control and lowering the possibility of illicit transactions under the Indian EFT system can be achieved by authorizing each EFT separately, giving the freedom to choose when along with whom your financial information is exchanged.[21]
3. **Data Security Measure:** DPDPA strengthens EFTs in India by requiring strong data security protocols. To protect sensitive data during EFTs, such as account numbers and transaction details, financial institutions must use robust encryption. As a result, even if data is intercepted, it becomes unintelligible, acting as a digital shield. Furthermore, access controls limit who within the organization has access to this data, reducing the possibility of internal misuse. Frequent security audits reinforce the defences even more and guarantee that these steps continue to be successful. EFTs operate in a more secure environment due to these DPDPA-enforced data security standards, which safeguard user privacy and financial information.[22]
4. **Right to Correction and Deletion:** The "right to correction and deletion" of personal data used for EFTs is granted to persons in India by the DPDPA.[23] This implies that people can ask the financial institution to make changes if any information related to an EFT transaction such as recipient information or transfer amounts is erroneous. Furthermore, if there are no regulatory or legal reasons to keep the data, the legislation gives the right to seek its complete deletion. This promotes more control over the data used in these financial transactions and gives people the ability to verify the correctness of their EFT data.[24]
5. **Data Breach Notification:** By requiring data breach notification, DPDPA improves the security of EFTs in India. The DPDPA requires financial institutions to quickly notify all

[20] Prakalp Sharma, 'State of Privacy in India' (Privacy International Aug. 2019) <https://privacyinternational.org/state-privacy/1002/state-privacy-india> accessed 12 February 2024.
[21] The Digital Personal Data Protection Act, 2023 (22of 2023) s 76(1).
[22] Soares Sallen, 'Data Governance in the Digital Age: How to Build a Data Governance Framework' (2023) 1(2) Data Governance Journal 135.
[23] The Digital Personal Data Protection Act, 2023 (22 of 2023) s 12 (1).
[24]George Hettich, 'Data Protection Frameworks in the Age of Big Data: A Comparative Analysis' (2020) 17 Greenleaf, G. Journal of Law, Information & Science 224.

 ISSN: 2582-6433

impacted parties in the event of a data breach that exposes personal information used in EFTs, such as account numbers or transaction details etc.[25]

(3.4) PENALTIES AND ENFORCEMENT MECHANISM

The DPDPA has penalties and enforcement measures in place to ensure compliance.

1. **Financial penalties:** The DPA has the authority to impose considerable financial fines on financial institutions that violate data protection legislation governing EFTs.
2. **Data correction orders:** The DPA has the authority to issue orders requiring financial institutions to correct erroneous personal data used in EFT transactions.
3. **Data processing restrictions:** In severe circumstances, the DPA may limit a financial institution's capacity to deal with personal data for EFTs until compliance is met.[26]

[25] Lina Jasmontaite, 'European Union: The European Data Protection Supervisor (EDPS) Opinion towards a New Digital Ethics' (2016) 2 Eur. Data Protection Law Review 93.
[26] The Digital Personal Data Protection Act, 2023 (22 of 2023) The Schedule.

 ISSN: 2582-6433

CHAPTER-4

Regulatory Framework and Judicial Activism of EFT in India

India's Electronic Funds Transfer system operates under a two-pronged approach: legal and regulatory.

(4.1) LEGAL FRAMEWORK

1. **Information Technology Act, 2000 (IT Act):** One of the most important factors in safeguarding EFTs in India is the IT Act 2000. How to do it is as follows:
    - **Encryption:** Although the IT Act gives the government the authority to enact regulations supporting secure communication practices, it does not specifically require encryption. This reduces the possibility of unwanted access even in the event that information is intercepted and subtly encourages banks and other financial institutions to encrypt critical EFT data (e.g. account numbers) during transfer.[27]
    - **Data Protection:** The IT Act contains rules for data protection; however, it is not as extensive as the more recent DPDPA (2023). It can be understood to protect personal information used in EFTs by forbidding illegal access, disclosure, or change of electronic records.[28]
    - **Intermediary Liability:** If intermediaries follow due diligence processes, the IT Act offers a safe harbor for them in order to prevent accountability for any illegal content or behaviour communicated through their platforms, intermediaries are encouraged to put strong security measures in place. Intermediaries, however, may be held accountable if they willfully aid in criminal activity or neglect to take down illegal content after being informed.[29]
2. **Negotiable Instrument Act,1881 (NI Act):** The NI Act 1881 provides some indirect protection for EFTs in India, even though its primary focus is on paper-based instruments. The definition of "cheque" in the Act is sufficiently broad to possibly include electronic checks that are utilized in some EFT systems as a substitute for cheques.[30] This provides legal remedy akin to that of bounced cheques in circumstances of dishonoured EFT transactions, which are rejected transfers because of insufficient funds. But one of the NI Act's shortcomings is that digital transactions aren't specifically covered.

[27] The Information Technology Act. 2000 (21 of 2000) s 84A.
[28] The Information Technology Act. 2000 (21 of 2000) s 43A.
[29] The Information Technology Act. 2000 (21 of 2000) s 79.
[30] The Negotiable Instrument Act, 1881 (26 of 1881) s 6.

 ISSN: 2582-6433

3. **Payment and Settlement System Act, 2007 (PSS Act):** A solid foundation for EFTs in India is established by the PSS Act of 2007. As the central authority, it appoints the Reserve Bank of India and gives it the jurisdiction to control and supervise EFT systems, including NEFT, RTGS, and IMPS. This guarantees efficient operation, safety, and equitable competition in the EFT market. In order to promote efficiency and trust in EFTs throughout India, the act also establishes the legal foundation for "netting" and "settlement finality," which states that an EFT transaction is final and cannot be reversed once settled.[31]

(4.2) REGULATORY FRAMEWORK

1. **Reserve Bank of India Guidelines (RBI):** The guidelines for secure and effective EFTs in India are established by the RBI. The operating structure for important systems like NEFT, RTGS, and IMPS is described in their "EFT Systems & Procedures" publication. By ensuring that all parties (banks) follow the same set of regulations, this promotes efficient processing and settlement of transactions. Furthermore, banks must adhere to strict cyber security regulations set forth by the RBI. This serves as a barrier, preventing unwanted access to sensitive EFT data, even in the event of cyberattacks. For India to continue having a safe and dependable EFT ecosystem, these RBI requirements are essential.[32]
2. **National Payment Corporation of India (NPCI):** With a focus on retail payments, NPCI is a key player in India's EFT industry. They oversee well-known platforms like UPI and IMPS, which let you send money via digital means like mobile banking. Your finances are managed by NPCI, but they work in the background. They establish the technical and functional requirements for these EFT systems, guaranteeing smooth bank-to-bank communication and promoting security. Consider them to be the unseen facilitator, ensuring that all participants work together to provide a safe and efficient EFT session.[33]

(4.3) JUDICIAL ACTIVISM

In **Umashankar Shivasubramaniam v. ICICI Bank,**[34] the complainant claimed that the bank's negligence resulted in the account being debited incorrectly, before the adjudicating authority

[31] Rajesh Rai and Tara Sivagnanasithi, Banking Theory- Law and Practice (2nd edn, Tata Mcgraw Hill Publishing Company Limited, New Delhi 2010).
[32] Electronic Funds Transfer System Procedural Guidelines, 2005.
[33] Roshan Kumar Mittal and Sanjay Dhingra, 'Technology in Banking Sector: Issues and Challenges' (2019) 27 (3) Indian Banking Publication 344.
[34] Umashankar Shivasubramaniam v. ICICI Bank (2010) 4 SCC 695.

 ISSN: 2582-6433

under the Information Technology Act in Chennai. ICICI argued that the case relates to phishing, and the customer is at fault for their own negligence and should submit a Federal Investigation Report. The bank also objected, claiming that the information was outside the scope of the IT Act of 2000.The adjudicating authority of the IT Act, 2000 found ICICI bank guilty of the offenses under Section 85 read with pertinent clauses of Section 43A, and ordered the bank to pay a total of Rs. 12,85,000. After submitting an appeal to the Cyber Appellate Authority, ICIC Bank was able to secure a stay on the judgement.[35]

In **State Bank of Mysore v. M/s. Venkatesh Prasad & Co.**[36] M/s. Venkatesh Prasad & Co. (the plaintiff), a corporation, experienced unlawful EFTs from its bank account. They sued the State Bank of Mysore (the defendant) for failing to protect their account and pay them for the losses they suffered. The case went to appeal and court acknowledged the bank's responsibility for providing a secure EFT system. However, they established an important concept: consumer contributory negligence. The court found that if a customer's fault clearly contributed to the unlawful EFT, the bank may be relieved of some or all liability. This case indicates that banks and customers share responsibility for securing EFTs. Banks must maintain strong security procedures, but clients must also exercise caution.[37]

In **Reserve Bank of India v. Canara Bank & Ors.**[38] the case strengthened the RBI's authority to supervise EFT systems in India. Prior to this case, the RBI's authority was challenged. This decision reaffirmed that the RBI has the legal authority to give directives and recommendations for the seamless operation, security, and consumer protection of the EFT ecosystem. This allows the RBI to establish standards for EFT systems such as NEFT, RTGS, and IMPS, assuring efficiency, security, and fair competition among participating banks. The RBI can also address issues including as settlement procedures, transaction fees, and dispute resolution systems. This case reinforced the regulatory framework for EFTs, promoting trust and stability in the Indian digital payment ecosystem.[39]

[35]Neeraj Arora, 'Phishing Scams in India and legal provisions' (ILP, 21 December 2020) <http://www.neerajaarora.com/phishing-scams-in-india-and-legal-provisions/> accessed on 13 March 2024.
[36] State Bank of Mysore v. M/s. Venkatesh Prasad & Co. (2017) SCC Online SC 223.
[37] Ibid 339,
[38] Reserve Bank of India v. Canara Bank & Ors. (2013) 10 SCC 732.
[39] Ibid 34.

 ISSN: 2582-6433

Chapter-5

Conclusion and Suggestions

India's EFT system is supported by strong legal frameworks and regulations. RBI establishes the foundation with rules for safe operating and safeguarding customers. Another layer is added by the DPDPA 2023, which requires financial institutions to have robust security procedures and gives users control over their EFT data. Further assistance is provided by extant banking rules such as the Information Technology Act, 2000 and the Negotiable Instruments Act, 1881. Together, these efforts create a safe environment. The secret is to remain vigilant at all times. Users must be informed of acceptable practices, and banks must be ahead of security concerns. India can secure a future in which EFTs enable businesses and people to engage confidently in the digital economy by placing a high priority on cooperation and education.

In order to protect sensitive data and data integrity, banks that use EFT systems and are becoming more computerized need to have a strong security strategy that outlines goals and system controls. For these measures to maintain high security standards, frequent monitoring, surveillance, and auditing are required. The security framework of systems and applications must be properly tested before being put into use, and upgrades must be made on a regular basis to provide improved security and control. Establishing Risk Management Cells with highly qualified staff to manage the different risks connected with online banking is a good idea, particularly for banks that conduct EFT.

Embracing biometric authentication methods such as fingerprint, face, eyes, voice recognition, and hand scans is critical, especially for rural communities, since they provide accuracy, mobility, and strong authentication. To effectively neutralize internal and external security threats, operating systems must be updated on a regular basis to prevent malware attacks, and the newest licensed software must be installed.

References

BOOKS

- Gurusamy S, Banking Theory- Law and Practice (2nd edn, Tata Mcgraw Hill Education Private Limited, New Delhi 2010).
- Rajesh R and Sivagnanasithi T, Banking Theory- Law and Practice (3rd edn, Tata Mcgraw Hill Publishing Company Limited, New Delhi, 2010).

 ISSN: 2582-6433

- Tannan ML and Gupta RN, ML Tannan Banking Law and Practice in India (Lexis Nexis 2017).
- Tannan ML, Tannan's Banking Law and Practice in India (23rd edn, LexisNexis India 2010).
- Uppal R K and Jatana R, E-Banking in India- Challenges and Opportunities (1st edn, New Century Publications, New Delhi 2007).

ARTICLES & LAW JOURNALS

- Ali Abdulah S.M, 'Legal Risk Associated with Electronic Funds Transfer' (2018) 17 (1) Plymouth Law School <https://pdfs.semanticscholar.org/3cd1/7d4de3b800a46aa07d55172c55096084058d.pdf> accessed on 11 March 2024.
- Chandra S, 'Electronic Funds Transfer: Exploring the Difficulties of Security' (2019) 5(4) Journal of International Commercial Law and Technology <https://media.neliti.com/media/publications/28771-EN-electronic-fundstransfer-exploring-the-difficulties-of-security.pdf> accessed on 11 March 2024.
- Chawla S and Singhal R, 'India and the World: The Changing Paradigms in the Banking Sector due to Technological Advancements' Prajnan, (2010) 6 (3) Law Journals Organisation.
- Hettich G, 'Data Protection Frameworks in the Age of Big Data: A Comparative Analysis' (2020) 17 Greenleaf, G. Journal of Law, Information & Science.
- Irfana S and Raghurama A, 'Innovation of Indian Banking: Extent of Precautions Taken by the Customers While E-Banking' (2013) 8 (5) IOSR Journal of Business and Management.
- Jaarsveld V, 'Domestic and International Bank Supervision and Regulation-Defying the Challenges' (2020) 119 (3) South African Law Journal.
- Jain S, 'Electronic Fund Transfers: A Critical Study in Indian Context with Special Reference to Security & Privacy Issues' (SSRN, 28 January 2018) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208110 > accessed on 12 March 2024.
- Jalal A, 'Evaluating the Impacts of Online Banking Factors on Motivating the Umamaheshwari Mahant., Savitri Sivasubramanian. & Harish Kumar, 'Online Credit Card Transaction Using Finger Print Recognition' (2010) 2(3) International Journal of Engineering and Technology 320- 322.

 ISSN: 2582-6433

- Mittal R.K and Dhingra S, 'Technology in Banking Sector: Issues and Challenges' (2006) 27(14) Indian Journal of Banking Institution.
- Mthembu M.A, 'Electronic Funds Transfer: Exploring the Difficulties of Security' (2018) 5(4) Journal of International Commercial Law and Technology, <https://media.neliti.com/media/publications/28771-ENelectronic-funds-transfer-exploring-the-difficulties-of security.pdf> accessed on 11 March 2024.
- Prakalp Sharma, 'State of Privacy in India' (Privacy International Aug. 2019)
- Sallen S, 'Data Governance in the Digital Age: How to Build a Data Governance Framework' (2023) 1(2) Data Governance Journal.
- Shukla SP, Rakesh N & Tyagi V, 'Problem Reduction in Online Payment System Using Hybrid Model' (2020) 3(2) International Journal of Managing Information Technology (IJMIT).
- Verma A, 'Phishing Attacks and perceptions of service quality: An Analysis of Virtual Banking in India' (2019) 3(1) AEIJST Journal of Management and Sustainability.

CASES

- Reserve Bank of India v. Canara Bank & Ors. (2013) 10 SCC 732.
- State Bank of Mysore v. M/s. Venkatesh Prasad & Co. (2017) SCC Online SC 223.
- Umashankar Shivasubramaniam v. ICICI Bank (2010) 4 SCC 695.