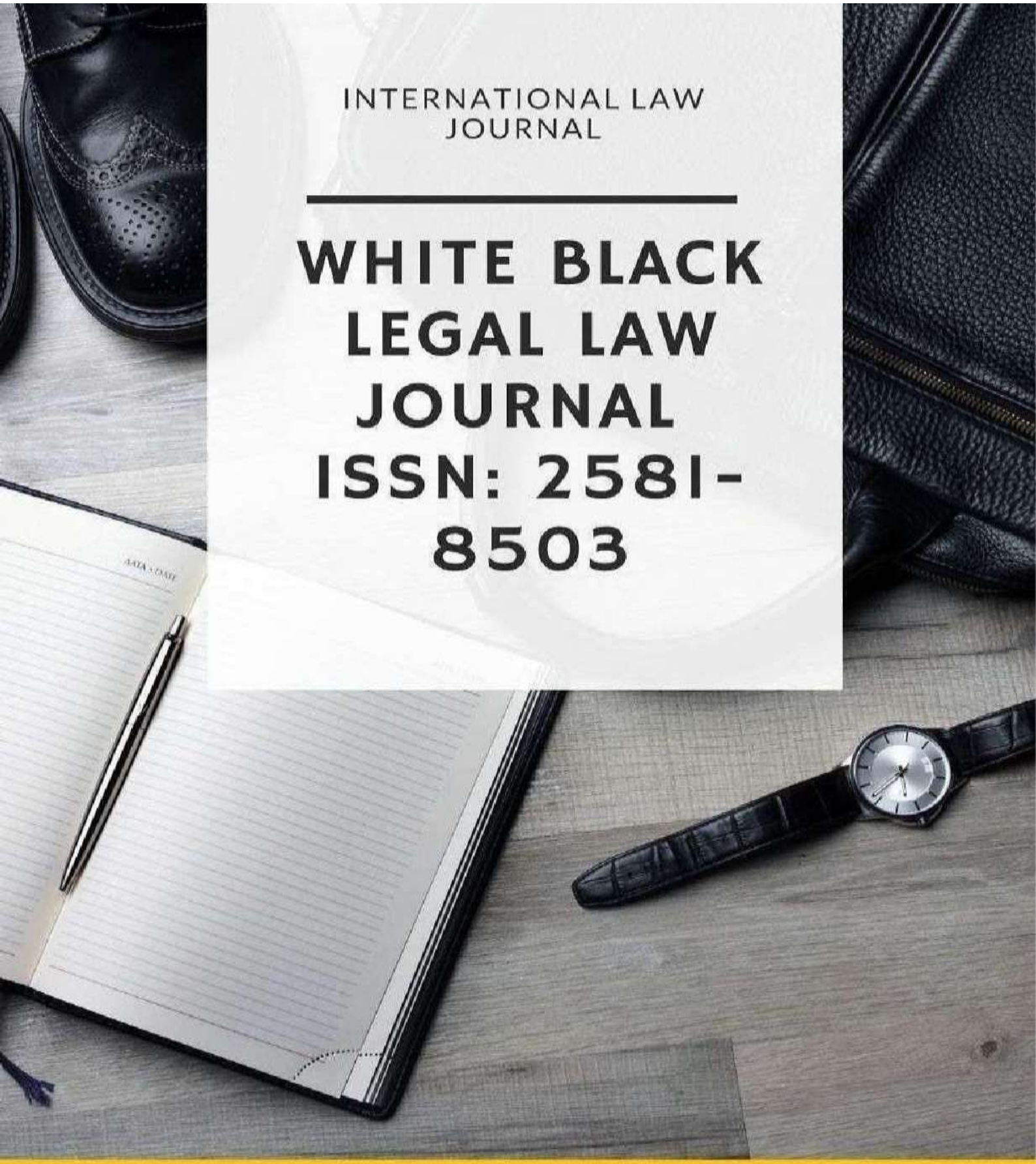

INTERNATIONAL LAW JOURNAL

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.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

E-BANKING FRAUDS - A CRITICAL STUDY OF THE LEGISLATIVE MEASURES

AUTHORED BY - SAKSHAM AHLAWAT
STUDENT, UILS, CHANDIGARH UNIVERSITY
CO- AUTHOR - DR. HARSHITA THALWAL
ASSOCIATE PROFESSOR, CHANDIGARH UNIVERSITY

Abstract

Modern times are marked by scientific and technological breakthroughs, and information and communication technology are a key factor in determining how society develops. It has an impact on many other areas, and the banking industry is no exception. Financial transactions have undergone a revolution with the introduction of e-banking, which makes it possible to transfer money seamlessly whenever you want and does away with the need to wait for regular business hours. E-banking has disadvantages, especially when it comes to security, even though it is quick and convenient. Despite its benefits, online banking has a considerable danger of serving as a conduit for illicit financial activity, such as frauds. People who carefully put money aside for unexpected expenses run the risk of being victims of e-banking fraud, in which dishonest individuals take advantage of several scams to accumulate fortune at the cost of the underprivileged. Current , most notably the Information Technology Act of 2000, as well as guidelines from regulatory organizations like the Reserve Bank, attempt to stop these illegal acts. The frequency of e-banking infractions keeps rising even with regulatory actions and the creation of a special complaint cell. Given the seriousness of the problem, thorough investigation is desperately needed to find workable answers. Researcher has directed their attention on scrutinizing pertinent laws in an attempt to gain understanding for tackling the growing problems related to online banking fraud.

Keywords

Financial, Legislation, E-banking, Technology, Frauds, Regulatory, Cyber, Framework, Digital, Services, Awareness, Bank, Cyber Security

Introduction

Almost every facet of our everyday lives has become digitized as a result of scientific and technological advancements. Large-scale banking sector changes were implemented in the early 1990s. Before 1980, banks only allowed customers to trade in person at physical branches. Customers now have the option to execute financial transactions through a variety of channels, providing a quicker option than manual banking, thanks to the reforms. Financial transactions may now be accessed with a single click. The banking sector has seen a significant transition as a result of this technical advancement. The provision of financial services via electronic channels is made easier by electronic banking, or e-banking. Foreign and younger private sector banks have been computerized from the start, in contrast to early private sector banks that were not entirely computerized.[1]

E-banking, or electronic banking, is a term for a system that uses computer and information technology to manage financial transactions instead of human personnel. E-banking functions without the bank and its customers having direct, in-person contact, in contrast to traditional banking services. Banks may easily give information and services to their consumers through e-banking by using a variety of platforms that are compatible with different terminal devices, such as desktop or browser-equipped mobile phones, digital televisions, and personal computers.[2] While electronic banking has many benefits, technological developments in the banking industry have also brought forth certain difficulties. In order to use e-banking services, one must overcome operational, technological, security, and regulatory obstacles. Users face several obstacles due to security issues, which include malware, illegal access, and data theft. Even while technology is advancing, the banking sector still faces several challenges, most of which are related to security and legal concerns.

The RBI, acting as a regulatory body, has released instructions to banks on combating fraudulent activity in response to the increasing number of cases of e-banking fraud. The financial institution is always modifying its policies to take into account shifting circumstances and protect against new types of fraud. It is critical to examine laws and policies relating to e-banking scams in order to solve the rising demographic issue in India and elsewhere. The successful enforcement of rules against e-

[1] Dr. C. Gupta and Abhilasha Sharma, "Banking Frauds in India: Trends and Legal Challenges", 03(01), *International Journal of Education, Modern Management, Applied Science & Social Science,* 276 (2021).
[2] Mrs. S. Kalpana and Dr. M. Mahalakshmi, "Cyber Crime: A Growing Threat to Indian E-Banking Sector", 7(12), *Journal of Emerging Technologies and Innovative Research* (2020).

banking fraud is contingent upon broad support, a point that is highlighted by the documented shortcomings in this regard.

Understanding E-Banking Frauds

The field of e-banking fraud is complex and includes a range of advanced methods that hackers use. Developing a sophisticated understanding of these fraudulent actions is essential to creating legislation that works.

- Phishing Attacks - Phishing is a common type of cyber fraud when people are tricked into disclosing private information like passwords, usernames, or bank account information by means of phony emails, texts, or websites. Phishing attacks in the context of e-banking frequently target gullible clients, sending them to phony banking portals where their login credentials are stolen illegally.
- Identity Theft - In the context of online banking, identity theft refers to the unlawful procurement and use of personal data in order to conduct fraudulent financial transactions. Armed with stolen identities, cybercriminals may take control of internet banking systems, putting both financial institutions and the affected individuals at serious danger.
- Malware and Ransomware - Ransomware and malicious software (malware) are sneaky instruments that cybercriminals use on victims. Systems become infected with malware, which compromises security and allows unwanted access to private information. Conversely, ransomware encrypts important data and demands a payment from hackers in order to decrypt it. Both provide serious risks to e-banking platforms, with the ability to impair business processes and expose consumer information.
- Account Takeover - When someone not allowed takes over a user's bank account, it's referred to as an account takeover in the context of e-banking fraud. This frequently happens as a result of stolen login information or holes in the authentication procedure. In addition to causing monetary losses for those impacted, account takeovers often reduce public confidence in the general security of online banking services.
- Insider Threats - Insider threats are malevolent acts carried out by members of an organization's own staff who take use of their special access rights to breach security. Within the realm of online banking, this may be a dissatisfied worker or a compromised employee working with outside

parties to enable fraudulent transactions. Because insider attacks originate in the secure setting of financial institutions, they present particular concerns.

E-Banking Legislation

The banking industry is seen as a key component in supplying the nation's financial needs. It is essential for promoting the growth and advancement of the country's economy. Through aggressively encouraging the public to save and invest, this industry has helped to keep money in circulation. These days, most people agree that banks are the main source of financial stability. However, it is reasonable to argue that the expansion of banking operations and people's growing reliance on banks to meet their financial requirements have contributed to an increase in fraudulent activity. These offenses include both offline and online fraud.

The widespread use of technology and the digital transformation of many industries have made life much easier. Like many other sectors of the economy, banking has adopted a number of technology innovations and services for its clients. A considerable percentage of banking activities have moved online. Even though technology has brought several advantages to the banking industry, fraud related to online banking has increased significantly in India. The following are some plausible contributing causes to the rise in e-banking fraud –

- The rise in online transactions throughout the previous ten years.
- A low level of customer awareness.
- Insufficient protection elements.
- Illicit hacking activities.
- Lack of strong data security protocols.
- Insufficiency of data security legislation.

The Reserve Bank of India Act of 1934, the Foreign Exchange Management Act of 1999, and the Banking Regulations Act of 1949 form the foundation of the legislative framework that governs banking in India. The major regulatory body in charge of approving bank licenses for all banks is the RBI. In short, as required by the Banking Regulations Act, 1949, any organization that wants to conduct business in India as a bank must first apply for and receive a license from the RBI. This

legislation specifies a number of tasks and prudential guidelines that banks need to follow. The Reserve Bank of India Act, 1934 deals with the laws governing non-bank entities that take public deposits. Furthermore, Indian residents are subject to limitations under the Foreign Exchange Management Act, 1999. Specifically, they are not allowed to borrow from or lend to non-residents, including non-resident banks, unless there are legally specified exceptions. In addition to these particular banking regulations, other trade and commerce-related enactments including the Indian Contract Act of 1872, the Negotiable Instruments Act of 1881, and the Indian Evidence Act of 1872 also have a big impact on how banking is conducted in India.[3]

Internet banking is seen as an extension of traditional banking, using the Internet to provide banking services and receive instructions from customers, as per RBI study on Internet Banking.[4] Essentially, Internet banking is theoretically expanded to fall under the same legal rules as traditional banking. However, the legality of online transactions and the usage of electronic media in general have come under intense examination. Electronic commerce and Internet banking are heavily impacted by important legal issues, including the legitimacy of electronic messages and documents, authentication, contract validity in electronic transactions, and non-repudiation. Because of the vulnerability of data and information transferred over the Internet, the research cast doubt on banks' ability to effectively comply with regulatory obligations pertaining to client account confidentiality, privacy, and consumer protection. Furthermore, there are legal gaps that make it difficult to handle technology-driven issues such data corruption or denial of service brought on by infrastructure or technology malfunctions, hacking, etc. Cross-border transactions made via the Internet also give rise to jurisdictional problems and legal disagreements between several countries.

Challenges in Combatting E-Banking Frauds

Technological Advancements and Cybercriminal Tactics

An age of extraordinary ease and efficiency has arrived in the modern environment with the widespread adoption of digital transactions. But in the middle of all the benefits that come with technical advancement, there has also been a noticeable increase in regulatory obstacles, which calls for a careful analysis of the complex dynamics that are involved in ensuring the security of digital

[3] Reserve Bank of India, "Chapter 7, Report on Internet Banking" (June, 2001).
[4] *Ibid.*

transactions. The prevention of fraud is a critical aspect of these regulatory difficulties. The integrity of digital transactions is always under risk from hackers' increasing sophistication, which calls for a regulatory structure that is alert and flexible enough to respond to their changing strategies. Regulatory organizations have the pressing challenge of strengthening defences against a variety of fraudulent activities, including identity theft and sophisticated cyber scams, as financial transactions move through digital channels.[5] Concurrently, the topic of data protection becomes a crucial focus point in the regulatory conversation. The enormous repositories of private data flowing over digital networks demand strict controls to protect user privacy and stop illegal access. The complex balancing act that regulatory frameworks must perform between enabling smooth digital transactions and guaranteeing strong protection of personal data necessitates a sophisticated strategy that takes into account the changing data security landscape. Furthermore, a major regulatory obstacle is the necessity of strong cybersecurity measures. Regulatory bodies are forced to create and implement strict cybersecurity policies due to the linked digital ecosystem's ever-growing attack surface. This includes a thorough framework that includes proactive threat detection techniques, safe authentication methods, and encryption requirements. For the regulatory environment to effectively protect digital transactions, it must be dynamic and constantly adjust to the new strategies used by cybercriminals.[6]

Jurisdictional Issues

A complex web of jurisdictional issues is created by the sophisticated and pervasive problem of e-banking fraud, which transcends national borders. The very nature of cross-border financial transactions introduces an additional level of complexity, making it more difficult to determine which legal jurisdiction should have jurisdiction over a particular issue. This uncertainty causes regular delays and complex legal problems by seriously impeding the timely and efficient prosecution of cybercriminals. To effectively handle the transnational aspects of e-banking fraud, a coherent and globally harmonized legislative framework is urgently needed. For a united strategy to be established in the fight against these complex crimes, international cooperation is essential. The lack of efficient international procedures frequently provides hackers with an opportunity to take advantage of legal gaps and evade accountability. Thus, in order to fortify the international reaction to e-banking fraud,

[5] Reserve Bank of India, "The Report of the Expert Committee on Legal Aspects of Bank Frauds" (September, 2001).
[6] Dr. Seema Modi, Ms. Vanshika Premani, & Ms. Mandeep Kaur, "A critical analysis of e-banking frauds and laws in India", 5(S2), *International Journal of Health Sciences*, 931 (2021).

it is essential to promote cooperation among states in the development and execution of all-encompassing legislative measures. It will need a concentrated effort to overcome the obstacles presented by disparate legal systems, various legislation, and discrepancies in law enforcement capacities between nations in order to create a strong and cohesive worldwide legal framework. This framework should set up procedures for coordinated investigations and prosecutions in addition to facilitating the effective exchange of information. Furthermore, addressing the challenges presented by disparate legal systems and cultural norms depends critically on developing a culture of trust and cooperation across states.[7]

Lack of Public Awareness

Dealing with the problem of e-banking fraud is quite difficult. This is mainly because most people are not aware of the many hazards and safeguards that come with online banking. Many consumers are not aware with the wide range of fraud strategies used by hackers, which leaves them open to identity theft and sophisticated phishing assaults. The need to educate people about the wide range of tactics used by cybercriminals is one of the main aspects of this difficulty. This include, but is not restricted to, social engineering techniques, malware assaults, and phishing attempts. Gaining a thorough awareness of these vulnerabilities is essential to enabling consumers to protect their online financial transactions in a proactive manner.

It becomes essential to promote the adoption of safe online habits in order to close the awareness gap that currently exists. One key component in improving the security of online transactions is two-factor authentication. Adding another line of defence against any fraudulent activity is educating users about the importance of routinely checking their account activities. The execution of educational programs and public awareness campaigns is shown to be a crucial tactic in reaching this objective. Along with highlighting the dangers of online banking, these efforts must to include detailed instructions for establishing and upholding safe online behaviours. Public service announcements, instructional seminars, and social media are just a few of the methods that may be used to efficiently spread this important information to a larger audience. In addition, cultivating cooperation between

[7] Dipti Gala, "E banking frauds a critical study of the Legislative measures", *Academia*, 2016, *available at* < https://www.academia.edu/68742316/E_banking_frauds_a_critical_study_of_the_Legislative_measures> (last visited on November 16, 2023).

governmental and financial entities is essential to developing a watchful and knowledgeable user population. Financial organizations may help by adding security features to their online portals and keeping people informed about any dangers. On the other hand, government agencies have the authority to establish and implement laws that support cybersecurity in the banking industry and provide a safe environment for online financial transactions.[8]

Coordination Among Regulatory Bodies

The complex environment around e-banking fraud highlights how important it is for various regulatory agencies entrusted with monitoring various aspects of the financial ecosystem to work together seamlessly. The varied nature of e-banking fraud adds to the complexity of this problem and calls for an all-encompassing, integrated strategy. In many cases, one of the biggest obstacles may be the lack of efficient coordination and communication between different regulatory bodies. These shortcomings make it more difficult to provide critical threat knowledge in a timely manner and create significant obstacles to the implementation of coordinated initiatives meant to successfully prevent fraud. Given the pressing nature of this issue, it is critical to improve collaboration between law enforcement and important regulatory organizations, like as the RBI.[9] To combat e-banking fraud, a coordinated approach involving the development of specialized task forces, strong information-sharing networks, and cooperative projects is required. In order to do this, regulatory agencies must to take a proactive role in creating and carrying out cooperative projects that improve the financial sector's overall cybersecurity posture. This cooperative approach will guarantee that a coordinated and proactive plan is in place to counter emerging threats in the quickly changing world of e-banking fraud, in addition to facilitating the smooth interchange of vital information. The success of these cooperative initiatives may also be greatly increased by establishing a culture of constant collaboration and communication through frequent meetings, workshops, and training sessions. Fostering a collaborative atmosphere where regulatory agencies cooperate, exchange knowledge, and collectively tackle obstacles might help the financial sector better adjust to the constantly changing strategies used by hackers to commit e-banking fraud.

[8] Ruchi Gupta, Shilpi Gupta, *et.al.* (eds.), *Electronic Banking Frauds: The Case of India*, 166 (IGI Global, 2023).
[9] *Supra* note 6.

The Way Forward

To strengthen the legal structure that deals with E-Banking frauds, it is necessary to carefully review and then update current legislation. This entails reviewing and revising laws, such the Information Technology Act of 2000, to make sure they remain applicable and effective in the face of changing cyberthreats. In order to speed investigations and prosecutions, proposed modifications should include measures that specifically target new types of E-Banking fraud, enhance penalties, and streamline legal procedures. Legislative efforts should also focus on developing a flexible and dynamic legal framework that can keep up with the ever-evolving tactics used by cybercriminals.

The complex nature of E-Banking fraud necessitates coordinated cooperation across several regulatory agencies. Strong channels for information exchange and coordination must be established by the RBI and other relevant institutions. This means setting up a single platform where information about possible risks may be quickly shared. Furthermore, encouraging cooperation between regulatory agencies and financial institutions would improve their combined capacity to identify, stop, and handle E-Banking fraud. Interagency cooperation of this kind is essential to the overall strengthening of the financial system.

Considering how important technology is to the commission and avoidance of E-Banking fraud, it is critical to strengthen cybersecurity protocols all the way around. To strengthen their defences against cyber-attacks, financial institutions should invest in cutting-edge technology like machine learning algorithms, artificial intelligence, and advanced encryption protocols. Furthermore, the danger of unwanted access may be greatly reduced by implementing multi-factor authentication methods. Financial institutions should be encouraged by legislation to implement and maintain cutting-edge cybersecurity procedures.

Moreover, industry-wide standards for E-Banking security should be developed by regulatory agencies working with cybersecurity specialists. Mandatory cybersecurity audits and evaluations for financial institutions will guarantee ongoing adherence to regulations and preparedness for ever-changing risks. Public awareness efforts can also stress the need of personal cybersecurity hygiene and encourage a shared accountability for safeguarding digital financial transactions. These

technology advancements and cybersecurity precautions, when combined with legislative frameworks, provide a strong barrier against the ever-present threat of E-Banking fraud.

Conclusion

Due to their simplicity, affordability, and ease of use, digital transactions are quite popular. On the other hand, because internet transactions are so simple, people are now more vulnerable to digital fraud. others of all ages clearly perceive that con artists are always looking for ways to defraud others of their money. Internet users must exercise caution while handling their personal data and be aware of their legal rights when using technology. Despite the presence of various legislation targeting e-banking fraud, their impact is limited. Robust and targeted legislation specifically created to combat e-banking scams is desperately needed. When used in combination with the Indian Penal Code, the Information Technology Act of 2000 only partially handles the legal actions pertaining to e-banking scams. The term "fraud" is not defined in the Indian Penal Code, thus digital financial scams are not sufficiently covered by it. Thus, in order to properly handle this issue, specific and thorough laws must be created. In order to fight bank fraud, the Reserve Bank of India regularly carries out research and publishes suggestions. Under the direction of Dr. N.L. Mitra, the Expert Committee on Legal Aspects of Bank Frauds suggested in 2001 that special laws be implemented in this area. Scams can only be avoided by raising public awareness, educating the populace, and fighting for user rights.