AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

SYSTEMATIC REVIEW ON DIGITAL BANKING AND PRIVACY OF DATA WITH SPECIAL REFERENCE TO INTERNATIONAL LAWS AND LAWS IN INDIA

Subhashis Chakrabartty
Research Scholar
20114281232046
Law
Dr. Kishwar Parween
Supervisor
Seacom Skills University, West Bengal

Abstract:

Digital Banking is the automation of traditional banking services. Digital banking enables a bank's customers to access banking products and services via an electronic/online platform. Digital banking means digitizing all of the banking operations and substituting the bank's physical presence with an everlasting online presence, eliminating a consumer's need to visit a branch. Data privacy is the ability of individuals to control their personal information. So, in this article systematic review on digital banking and privacy of data with special reference to international laws and laws in India has been discussed.

Keywords: Digital, Banking, Privacy, Data, Laws.

INTRODUCTION:

Digital financial refers to the automation of conventional financial services. Digital banking allows users to access banking goods and services through an electronic or online platform. Digital banking entails the digitization of all banking processes, replacing the physical presence of banks with a perpetual online presence, hence obviating the necessity for consumers to visit a branch. Digital banking allows consumers to execute banking transactions from the convenience of their

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

homes, whether it be an elderly individual weary of queuing, a working professional preoccupied with duties, or an ordinary person wishing to avoid a trip to the bank for a singular task. It additionally provides convenience. Digital banking enables users to establish automatic payments for recurring utility bills, including energy, gas, telecommunications, and credit card obligations. The customer is no longer required to consciously recall the due dates. The consumer may choose to receive notifications regarding forthcoming payments and outstanding balances. The expansion of digital financial services to rural areas appears to be a move toward comprehensive growth. The rural populace may fully utilize digital banking services due to the availability of affordable cellphones and internet connections in remote regions.

SYSTEMATIC REVIEW OF LITERATURE (STUDIES CONDUCTED IN INDIA):

Roy, D. & Lohana, S. (2024). Preventing and detecting fraud is a national priority. The national economy's corporate image depends on the prevention of fraud, which calls for stringent prosecution in addition to an effective system to detect and halt frauds in progress. This study investigates the forms and nature of bank frauds, their effects, and the bank's perspective on the variables that lead to bank frauds, the regulatory environment, and strategies for preventing fraud. We gathered secondary data on bank frauds from 2004–05 to 2022–23 from the RBI website to determine the correlation between the various bank fraud categories. We questioned other bank administrators to understand the techniques used by fraudsters and their defense. We conducted an interview to gather information about the Nirav Modi case, which serves as the foundation for our case study analysis. This study also examines the shortcomings of the bank's operational risk architecture. It also aims to review the risk management architecture in banks and offer suggestions to stop bank fraud events based on the analysis and conclusions.

Bhargavi, C. & Sravanthi M. (2023). Financial fraud is on the rise as a result of banks moving their operations to digital platforms. For banks and other financial institutions, fraud is a serious problem. Scammers exploit system weaknesses to lose billions of dollars annually. For this reason, having robust fraud detection processes in place is essential. Fraud is a serious problem that affects banks, businesses, and people in general. Thankfully, the financial industry can utilize a few digital

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

technologies to identify and thwart fraud. This study emphasizes how using technology like artificial intelligence, multi-factor authentication, machine learning algorithms, and fraud detection software may help banks and businesses protect themselves and their customers against criminals. According to 63 percent of financial institutions, artificial intelligence (AI) technology is excellent at spotting scams and can even stop cybercrime before it starts.

Gupta, R., Gupta, S., Ajekwe, C.C. (2023). Developing nations have benefited greatly from the invention and commercial expansion of electronic banking, or "e-banking." E-banking accelerates the growth of the capital markets, digital economy, and financial industry. India's rapidly expanding banking sector has facilitated the development of the e-banking regime and fraud prevention. The goal of this chapter is to evaluate fraud detection methods on a worldwide scale while also validating the rise of online banking with caution and knowledge. We have gathered secondary data from journals, the internet, and bank records. The findings will improve the current fraud protection systems and aid banks and regulators in understanding online banking scams. The government should encourage widespread adoption of information and communication technology for positive impacts, while also ensuring adequate infrastructure in the energy and telecommunications sectors.

Kirti, K. (2023). Information technology has made it possible to conduct most banking tasks while enjoying a cup of coffee or engaging in meaningful discussions. You can easily find ATMs at your door these days, and banking services are available around the clock. More plastic cards than monetary notes are in circulation. The extremely globalized, liberalized, privatized, and competitive environment in which banks operate today is primarily responsible for this enormous shift. Banks must use IT to stay afloat in this difficult environment. As a result of significant advancements in IT, the Indian banking sector has experienced remarkable growth. In this context, electronic banking, or "e-banking," has emerged as a revolutionary development. The purpose of this article is to examine and assess the advancements achieved by the Indian banking sector in using this technology. This analytical study examines a number of ebanking-related characteristics, including branch computerization, automated teller machines, and transactions made through retail electronic payment methods. It does this by using secondary data. We analyse the data using

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

statistical and mathematical methods, which include averages, growth rates, and percentages. This study shows that, although e-banking has many advantages for both people and businesses, there are drawbacks, including concerns about consumer security and interests. Several studies have examined the success of e-banking on various scales, but only a handful have conducted a thorough and methodical analysis of the Indian banking industry. As a result, this paper will highlight numerous e-banking system features from the perspective of a researcher and point out any research gaps that are unique to the Indian setting.

Sharma, K.N., Kala, A. (2022). The banking sector has experienced significant digital upheaval. E-bill payments, smartphone apps, and online banking are now standard. Banking digitalizes the process from the back end to the front end, eliminating the need for human intervention in transactions. While speed is the fastest aspect of digital banking, is it consistently reliable? Cybercriminals can easily compromise online transactions due to ignorance or careless errors. The goal of this study is to examine online banking fraud, including phishing, smishing, card fraud, and other related crimes, as well as their root causes. We conducted interviews with bank employees to understand their perspectives on these frauds and whether they are involved in any fraudulent operations. Finally, a model of the fraud detector system and, by extension, the preventative measures that can assist a person in keeping safe from online scams have been attempted to be built.

Khan, M.S. & Savitvh, J. (2022). The financial sector is essential to the expansion of a nation's economy. Banking is the lifeblood of an economy. An active and well-resourced financial sector is necessary for economic growth. An IT revolution is currently occurring in the Indian banking industry. The execution procedure. The banking sector has seen a change thanks to the advent of the internet. It has yielded positive results. It was advantageous to banks as well as customers. E-banking has become more and more common in India. Thanks to innovation and technical breakthroughs, there have been several changes. The financial sector has undergone several changes. The word "e-banking" refers to a wide range of services. This term encompasses various services such as online shopping, fund transfers, and mobile banking. Through e-banking, the bank intends to provide fundamental IT knowledge. Included services with an Internet foundation.

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

Customers find it more convenient to make debit payments under the traditional banking system. in addition to credit One of the reasons e-banking is becoming more and more popular in India is because more people are using the internet. With so many advantages, online banking is gaining traction. There is a connection to it. It has, nevertheless, brought up several issues and challenges. In terms of cybercrime, which includes credit card fraud, phishing, and data theft, this article aims to give an overview of electronic banking in India along with the various issues and difficulties that the banking industry faces.

Modi, S., Premani, V., & Kaur, M. (2021). This is the current era of science and technology. Technology and information exchange have a significant positive impact on society. It has benefited every aspect of society. This also applies to the banking industry. Thanks to e-banking, you can move money at any time without waiting for bank openings. Therefore, e-banking is very quick and easy. But there's a downside to internet banking. It's not entirely risk-free. Scams in e-banking illicitly transfer substantial amounts of money. The average impoverished man works extremely hard to save money for emergencies, yet online bank scammers use every trick to get cash fast and take advantage of the weak. Authorities have implemented laws to regulate it. The Information Technology Act of 2000 provides concrete evidence of this. Moreover, the Reserve Bank promptly issues directives in this regard. The Reserve Bank has established an independent complaint unit to address these grave issues. On the other hand, evidence suggests that these offenses are getting worse every day. It is crucial to investigate and find a practical solution to this issue.

Kavita (2021). The Indian financial system could go cashless through Internet banking. People frequently refer to internet banking using terms such as "e-banking," "online banking," "virtual banking," or similar terminology. A payment gateway is an "electronic payment system" that enables customers of banks or other financial institutions to conduct a range of financial transactions through their websites. "Core banking" encompasses a range of online financial transactions such as Nation Electronic Fund Transfer (NEFT), real-time gross settlement (RTGS), electronic clearing system (ECS), immediate payment service (IMPS), automated teller machine (ATM), smart cards, and telebanking. Using Internet banking services, we can check our accounts

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

whenever we want or as often as we'd like, day or night. In recent years, the frequency of internet banking frauds in India has increased dramatically. India does not yet have enough laws pertaining to online banking. The RBI recently released some guidelines in this area; however, they are insufficient to guarantee banks follow the essential and stringent cyber safety protocols. The article discusses the latest advancements in online banking, including concerns about cyber security and its advantages and disadvantages. It also discusses the legal framework that India has put in place to shield its citizens from identity theft and cybercrime.

Johri, N. (2021). The goal of this paper is to provide an overview of online banking scams in India, including statistics, security dangers associated with them, legislative frameworks governing e-banking, and RBI suggestions for mitigating risk associated with e-banking. Since e-banking has emerged as the industry's new trend in banking, it is critical to take into account the system's vulnerabilities and potential for fraud. Before concluding this essay, I'll provide some guidance on preventing online banking scams.

Thakur, S. (2019). This study looked at the types of electronic banking fraud that affect deposit money banks in India, as well as the safeguards put in place to stop financial loss. The growth of online banking, primary pathways for cybercrime, factors contributing to the elevated frequency of fraud, and forms of cybercrimes that utilize computers and information and communication technology to deceive banks were all examined in this study. The study used a case study research design, which relied on secondary data collection methods. The Indian Electronic Fraud Forum (NeFF) Annual Report 2016 is the main topic of the article. According to observations, there were 19,531 fraud incidents registered in 2016 compared to 10,743 in 2015, an 82% rise. However, there was a slight decrease in the value of real loss and attempted fraud. The study found a strong correlation between India's e-banking habits and the rate at which banking transaction security is improving. The number of financial transactions has dramatically increased as a result of the adoption of e-banking. Additionally, it has made customer service delivery easier and better. The study demonstrates that the impact of electronic fraud will lead to the loss of funds that belong to the bank or its clients. Among other consequences, it could potentially damage the bank's reputation. The researcher came to the conclusion that electronic banking has security issues, but

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

it has increased bank operating efficiency in India. The researcher recommends, among other things, that the government, through the CBN, provide adequate security measures for various electronic banking channels, assess the BVN framework, and educate clients about electronic banking operations in light of these findings.

SYSTEMATIC REVIEW OF LITERATURE (STUDIES CONDUCTED ABROAD):

Aljudaibi, S.A., Amuda, Y.J. (2024). The rapid expansion of digital banking services in Saudi Arabia makes it abundantly evident that thoughtful legislative judgments are essential. Nonetheless, there remains uncertainty about how to use the legal system to safeguard consumer rights and establish a trustworthy environment for digital finance in the Kingdom's digital banking industry. The primary objectives of this study are to scrutinize the legal framework in Saudi Arabia that safeguards digital bank customers, and to evaluate its methods, content, and impacts on different stakeholders. In a similar vein, the study looks for obstacles that might stand in the way of its success as well as its effectiveness. The evaluation finalizes comments about the legal sector and outlines important concerns and challenges through a thorough analysis and examination. The content analysis approach addressed issues arising from the body of current literature. We examined numerous academic journals, policy papers, and regulatory standards. In other words, we gathered data for this study from a variety of search sources such as journals, standard Google Scholar articles, policy papers, and library resources. We examined a total of twenty-five publications, which significantly contributed to revealing different facets of the Kingdom's consumer protection laws and the legislative framework surrounding digital banking. The investigation's findings identified three main issues with Saudi Arabia's domestic law control of consumer protection in the country's digital banking system. First, the study examined a number of laws pertaining to the rights and obligations of consumer protection, including sector-specific regulations and consumer protection laws. Second, there are legal requirements for pursuing remedies in cases of discriminatory treatment in online banking. Third, it is clear that Saudi Arabia has moved proactively to minimize the risks associated with cybersecurity in the country and to provide a strong safety net to defend consumer rights. On the one hand, the study theoretically

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

emphasizes how important it is for the Kingdom to have laws protecting consumers. However, given the Kingdom's rapid economic expansion and technological advancements, it is more crucial than ever to implement robust consumer protection laws to foster consumer confidence in the marketplace, promote ethical business practices, and foster trust. However, the identification of significant shortcomings, such as inadequate consumer education and regulatory shortcomings, necessitates national coordination among stakeholders. Prompt review, revision, and enforcement are considered essential for resolving new problems and attracting customers to digital banking, even if the legal structure performs well in addressing important issues.

Ahmad, I., Khan, S. and Iqbal, S. (2024). This study endeavors to scrutinize and evaluate the banking sector's adoption of digital technologies and their impact on the proliferation of digital fraud, specifically focusing on online banking scams. This study looks at the strategies employed by cybercriminals to take advantage of security flaws in online banking systems and attempts to shed light on the technologies that banks are currently using to secure them. This research did a systematic literature review (SLR) on digital banking, online banking fraud, and security metrics in order to understand how digital technologies in banking might be safeguarded against online fraud. The review encompasses a wide range of online databases such as Emerald Insight, Google Scholar, IEEE, JSTOR, Springer, and Science Direct. The paper's main conclusion is that the banking industry's embrace of digital technologies has significantly increased the amount of digital fraud, especially online banking scams. Cybercriminals in this industry, which has become a global concern, employ sophisticated tactics such as phishing attempts, denial-of-service assaults, Trojan horses, malware infections, identity theft, and computer viruses. The use of digital technologies in the banking sector and its relationship to the rise in online fraud are the main topics of this study. One unique feature is the emphasis on the relationship between technology and fraud in the financial industry. This study uses a systematic literature review (SLR) to investigate the technologies that banks are currently using to secure their online banking systems. This thorough approach offers insights into the range of security measures banks employ to guard against different kinds of cyber threats.

Phiri, J., Lavhengwa, T. & Segooa, M.A. (2024). The banking industry offers online banking so that its clients can easily and conveniently access financial services. Since the majority of banking

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

services are now handled online, worrying fraud occurs on a regular basis. Globally, internet banking frauds are becoming more frequent and widespread, posing a significant threat to both banks and clients. The aim of the study was to examine problems with online fraud detection in the banking industry in South Africa and Spain. The study employed the Design Science Research (DSR) technique. We gathered the data using the qualitative method, particularly through focus groups and semi-structured interviews. We used non-probability sampling because the study focused on a specific subset of online fraud models. The overall population consisted of 17 participants, including data scientists, fraud technical managers, fraud investigators, and fraud technical specialists. The survey revealed a shortage of internet fraud specialists within the banking industry in South Africa. The results show that banks may have inadequate detection systems as a result of a lack of experience with online fraud. The report indicates a significant likelihood of legal regulation gaps from a Spanish perspective. The banking industry urgently requires internet fraud specialists, prompting banks to cultivate and acquire such expertise. Online banking technology is advancing faster than traditional transaction methods, necessitating frequent changes to rules and guidelines to keep pace with these rapid technological advancements. The study recommended topics that the banking industry may look into to build and improve online fraud detection models in order to combat online fraudulent activities, given the relevance of global online banking.

Ramya, R., Raj G, S.M. (2024). In the digital age, online fraud has become an inevitable threat that poses serious risks to individuals, businesses, and financial institutions all over the world. This article examines the realm of online banking scams, highlighting common categories, flaws, effects, and effective remediation techniques. Malicious activities such as phishing, virus attacks, fraud, account takeovers, credit card fraud, and social engineering schemes are examples of online banking scams. These tactics make use of flaws in customer behavior, security norms, and online financial frameworks to cause financial losses, damage to one's reputation, and breaches of trust. Online fraud affects people's security, trust in online transactions, and the stability of the financial biological system in addition to causing financial hardships. The potential for severe suffering, legal ramifications, and long-term financial effects for victims of internet frauds emphasizes how important it is to address this unavoidable risk. To enforce relief measures against online fraud,

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

we need a multifaceted approach that includes administrative, mechanical, and conduct intercessions. To keep online financial systems and customer data safe, financial systems should have strong network security features like encryption, multimodal verification, continuous exchange monitoring, and extortion identification algorithms. This article covers the laws in the USA and India pertaining to internet banking fraud.

Vanini, P., Rossi, S., Zvizdic, E. et al. (2023). When a criminal is able to control an account and move money out of a person's online bank account, it's known as online banking fraud. Finding as many fraudsters as possible and minimizing the number of false alarms raised is crucial for effectively stopping this. Machine learning has difficulties because of the highly skewed data and intricate nature of fraud. To minimize anticipated financial losses, it is also necessary to enhance traditional machine learning techniques. Finally, understanding the costs and risks associated with payment methods is essential to fighting fraud in a methodical and cost-effective manner. We provide three models that address these issues: a risk model that forecasts the likelihood of fraud while taking preventative actions, machine learning-based fraud detection, and economic optimization of machine learning outcomes. We tested the models using real data. Compared to a benchmark of static if-then rules, our machine learning model alone reduces the predicted and unexpected losses in the three aggregated payment channels by 15%. Further refinement of the machine-learning model reduces the predicted losses by 52%. With a low false positive rate of 0.4%, these results remain valid. From a commercial and risk standpoint, the three models' risk framework is therefore workable.

Găbudeanu, L. et al. (2021). Over the past ten years, the market's specialty literature and products have concentrated on gathering and combining huge volumes of transaction (and user) data as well as improving the algorithms that detect fraud. Simultaneously, the European Union has enacted laws, such as PSD2, that follow a similar path and require stakeholders to recognize fraudulent activity. On the one hand, the legislation provides a broad outline of this legal requirement, while on the other hand, the market is witnessing a growing diversity in the data solutions available, particularly in their efforts to combine data for more precise outcomes. The topic of privacy concerns associated with creating profiles and aggregating data for fraud identification, and the accountability of stakeholders for fraud identification in light of their duties under data protection

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

laws, remains unexplored in specialized literature or by lawmakers. This article, by analyzing current fraud detection techniques and approaches, considering their implications for data protection laws, and examining respondents' attitudes toward privacy when identifying fraud in transactions, serves as a foundation for further research in this area. The analysis is based on a survey with 425 respondents. Thus, by offering suggestions for both complying with the legal responsibility of fraud detection and adhering to data protection issues, this article helps close the gap between data protection legislation and its implementation.

Kjorven, M.E. (2020). Identity theft and other forms of online financial crime that target consumers are becoming more common. The financial institution or the customer often bears the loss, as recovering losses from the fraudster can be a challenging task. This article's study focuses on how these two parties should allocate losses from online financial fraud in compliance with applicable European and Scandinavian law. National rules govern loss allocation in payment-transaction fraud, implementing the payment services directive's responsibility system for unauthorized payment transactions. Ordinary contract and tort laws provide answers to these questions about other financial services. The data demonstrates that victims of online financial fraud frequently have to bear the consequences of their losses. One argument is that the financial services sector's digitalization has actually changed who is responsible for attacks on financial institutions. This goes against the declared policy objectives of the EU to offer robust consumer protection against cybercrime. The study comes to the conclusion that financial institutions ought to bear a greater share of the damages caused by online financial fraud.

Ali, M.A. et al. (2019). In addition to offering consumers more satisfaction through higher-quality services, e-banking gives banks a competitive edge over other industry participants. However, the fraudulent actions of fraudsters have drawn attention to the security of e-banking; the lack of sufficient protection has prevented many users from using the service up to this point. This paper provides an overview of the security issues related to online banking. This paper replicates the challenges and characteristics of online banking fraud. This study also examined various fraud and attack detection systems and the safeguards put in place to protect e-banking services. This study ranked the various e-banking security models and methodologies based on expert opinions. The best model, according to the results, was "transaction monitoring," whereas the worst models, in

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

the respondent's opinion, were "virtual keyboards," "browser protection," and "device identification." The first section of this article provides an overview of the issue of interest, while the second section provides background information on e-banking. The third section of the document contained the literature review, and the final section had the conclusion.

CONCLUSION:

The underlying presumption on digital banking is the convenience the users are willing to have. With the options as to e-banking, fast money transfer the consumers are now dependent in their entirety. The growth in commerce and industry more fully e-commerce has widened up due to the utilization of such facilities but the drawbacks lie enormous and such challenges need to be addressed. Phishing, Proofing, Fraud and identity theft are common in such transactions. The confidential data and money from such accounts are being enticed away by crooks. Several studies have come from different researchers showing the problems and the guidelines framed by controlling authorities more specifically the Reserve Bank of India and the notifications issued by the Ministry of Information and Broadcasting, Government of India. The researches have failed to address the problems like failures in third party security systems used by different banks. The areas like transaction speed, lack of computerization, security threats are challenges. The platforms are colliding in nature and no specific forums have been formed to address such colliding instances, even in international level. Moreover, the fast-changing nature of cyber-crime industry and lack of individuals' knowledge encourage its consistent expansion. The damage caused by worldwide cyber-crimes is estimated to cost $10.5 trillion per year by 2025.

REFERENCES:

1. Ahmad, I., Khan, S. and Iqbal, S. (2024). Guardians of the vault: unmasking online threats and fortifying e-banking security, a systematic review, *Journal of Financial Crime*, 1, 1-18.
2. Ali, M.A. et al. (2019). E-Banking Fraud Detection: A Short Review. *International Journal of Innovation, Creativity and Change*, 6(8), 67-87.
3. Aljudaibi, S.A., Amuda, Y.J. (2024). Legal framework governing consumers' protection in digital banking in Saudi Arabia. *Journal of Infrastructure, Policy and Development*, 8(8), 1-18.

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

4. Bhargavi, C. & Sravanthi M. (2023). Significant Role of Digital Technology in Detecting Banking Frauds in India. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(3), 1124-1127.
5. Găbudeanu, L. et al. (2021). Privacy Intrusiveness in Financial-Banking Fraud Detection. *Risks*, 9(104), 1-22.
6. Gupta, R., Gupta, S., Ajekwe, C.C. (2023). Electronic Banking Frauds: The Case of India. *Theory and Practice of Illegitimate Finance*, 1, 166-183.
7. Johri, N. (2021). E-Banking Frauds and Safety Solutions: Analysis. *Indian Journal of Integrated Research in Law*, 2(6), 1-12.
8. Kavita (2021). Analysis of Internet Banking along with Legal Aspects in India. *Kurukshetra Law Journal*, 11, 113-129.
9. Khan, M.S. & Savitvh, J. (2022). Legal Perspective of E-Banking Fraud in India. *International Journal of Innovative Research in Engineering & Management*, 9(2), 214-218.
10. Kirti, K. (2023). Analytical Study of E-Banking Frauds and Its Impact on Indian Economy. *International Journal for Legal Research & Anlaysis*, 2(7), 5-20.
11. Kjorven, M.E. (2020). Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe. *European Business Law Review*, 31(1), 77-109.
12. Modi, S., Premani, V., & Kaur, M. (2021). A critical analysis of e-banking frauds and laws in India. *International Journal of Health Sciences*, *5*(S2), 931–938.
13. Phiri, J., Lavhengwa, T. & Segooa, M.A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, 26(1), 1-8.
14. Ramya, R., Raj G, S.M. (2024). Laws Regulating Online Banking Frauds in India: A Comparative Study with Existing Laws in USA. *Aut Aut Research Journal*, 14(5), 1-15.
15. Roy, D. & Lohana, S. (2024). Bank Frauds in India: Trends, Modus Operandi and Preventive Measures. *National Institute of Bank Management WP*, 1, 2-6.
16. Sharma, K.N., Kala, A. (2022). Online Banking Frauds and Necessary Preventive Measures. *International Journal of Commerce and Management*, 16, 50-57.
17. Thakur, S. (2019). Electronic Banking Fraud in India: Effects and Controls. *International Journal of Science and Research*, 8(10), 823-829.
18. Vanini, P., Rossi, S., Zvizdic, E. et al. (2023). Online payment fraud: from anomaly detection to risk management. *Financ Innov*, 9(66), 1-25.

AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume: 3 Issue: 3
September 2024
Impact Factor:11.9
Subject: Law

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds Any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Subhashis Chakrabartty

Dr. Kishwar Parween

*****