INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

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

E-BANKING FRAUDS: UNVEILING THE THREAT OF 'INSIDER RISKS'

AUTHORED BY - KRISHANGEE BHATTACHARYYA,
Advocate (presently practicing at The Gauhati High Court),
LLM, Symbiosis Law School, Hyderabad, Symbiosis International (Deemed) University,Pune, India, B.A LL.B (Hons), National Law University and Judicial Academy, Assam.

Abstract

The frauds at banks are more dangerous because a huge portion of populace trusts them with holding their money and deposits. Although e-banking has numerous benefits, it has also given scammers many opportunities to exploit its flaws and difficulties to execute cunning fraudulent practices that cost institutions a lot of money. The misuse of personal details without authorization, problems with data access, a lack of awareness of data security among both consumers and staff members, money laundering, and regulatory issues are just a few among thelawful, compliance, safety, and operational challenges that are presented by evolving e-banking systems. The dangers associated with e-banking systems impact the banks in regards of damagesto their finances and reputations, necessitating ongoing policy reviews from the legislation, authorities, and administration. The review of the literature finds that there has been relatively little research on insider risks in e-banking services, and that existing legislation and rules donot sufficiently prohibit fraudsters.

Thus, the researcher, in this study will focus on current fraud trends in the e-banking industry and will also include a thorough examination of insider risks associated with e-banking fraud as well as the effectiveness and efficiency of the current legislative framework around the aforementioned issue.

Keywords: *E-banking, frauds, online banking, technology, insider risks, fraudulent, fraudsters, consumers*

 ISSN: 2582-6433

Introduction

In the recent years, the banking sector of India has experienced enormous expansion. Over the past two decades, the banking industry has entirely changed from manual to computerized transactions. Automated Teller Machines (ATM), Internet and Mobile Banking, and most recently Payment Gateways and Aggregators have altered how people bank today, making it easier to access banking services and give customers additional payment methods.[1] Globalizationand constantly advancing technologies have, however, dramatically changed the fraud scene in India and around the world as well. The more conventional means of fraud have been replaced by newer ones, raising concerns regarding regulation and prevention. The amount of fraud activities, both internal and external, has increased as a result of technological advancements in the way banking is conducted today. In addition to online banking, India has seen impressive growth in sectors like mobile banking, payment banks/aggregators like PayTM, payment gateways like Citrus Pay, CC Avenue, etc., all of which have increased the risk of fraud while facilitating easy access to banking activities and other payment options.[2]

The recent years has witnessed a growth in the use and acceptance of different modes of E- banking which has increased the frauds involving banks, both internal and external. The alternative modes of banking have paved the way for scammers to take advantage of the built-in flaws in technology-based banking systems. The security of the data of the customers is one of the most vulnerable aspects of online banking. Customers' sensitive personal information is stored by banks, and any unauthorized access to or use of that information is a severe problem, especially since many bank workers have access to that information and could use it improperly or manipulatively. Most investigations indicate that top management in addition to mid-level personnel have been in these frauds. The amount of money lost to fraud and the number of fraudsstill being committed have not decreased despite different laws that have been passed and actionstaken by the RBI over the past couple of decades. This tendency raises major questions about theefficiency of policies of enacted by the RBI and the Government of India as well as the

[1] Dr. S. Venkata Ramana & Dr. S Gopi Krishna, *A study on impact of fraud in Indian Banking Sector (with special reference on retail banking product)*, 2 (6) INT'l J. of Academic Research and Development, 15 (2017), http://www.academicjournal.in/archives/2017/vol2/issue6/2-6-250.
[2] Parisha Singh, *Online Banking Frauds and Role of Government to Curb It: With Special Reference to India*, 3 SUPREMO AMICUS 365 (2018).

 ISSN: 2582-6433

effectiveness of measures for detection and prevention, which has further emphasized the need for a review of the current legislative framework.

Significance of the Study

Because so many people trust banks to store their cash and savings, bank scams are especially harmful. Although e-banking has many advantages, it has also given scammers ample chances to take advantage of its shortcomings and challenges to carry out devious fraudulent practises that cost banks a lot of money. A few of the legal, compliance, safety, and operational obstacles posed by developing e-banking systems include the unauthorized use of personal information, issues with data access, a lack of understanding of data security among customers and employees, money laundering, and regulatory issues. The legislation and rules controlling them are not developing at the same rate as technology, which is advancing quickly, and the systemson which E-Banking service are being supplied. The current research focus on current fraud trends in the e-banking industry and will also include a thorough examination of insider risks associated with e-banking fraud as well as the effectiveness and efficiency of the current legislative framework around the aforementioned issue.

Review of Literature

In order to research on the aforementioned issue, the researcher has reviewed the following literature.

B. R Sharma[3] in his book summarizes the types of banking frauds that exist, how they operate, and what can be done to stop them and lessen the harm they inflict. **Ashu Khanna and Bindu Arora**[4], in their paper, evaluated the various factors that contribute to bank frauds. It attempts to shed light on bank workers' attitudes toward preventive measures and their awareness of various scams. The paper also highlights the importance of training in bank fraud prevention. **Usman**

[3] B.R SHARMA, BANK FRAUD: PREVENTION & DETECTION (Universal Law Publishing Co. Pvt. Ltd. 2009).
[4] Ashu Khanna & Bindu Arora, *A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry*, 4(3) INT'l J. of Business Science and Applied Management,1 (2009), https://www.business-and-management.org/library/2009/4_3--1-21-Khanna,Arora.pdf.

 ISSN: 2582-6433

Kabir Ahmad & Mahmood Hussain[5] were of the view that weak firewalls, ineffective internal controls, inadequate authentication protocols, and weak security systems are the main causes of frauds in e-banking. They stated in their paper that to lessen fraud and fraud risks in E-Banking, effective security controls must also be implemented. **Sukanya Kundu & Nagaraja Rao**[6]**,** through their study, have come to the conclusion that there are several factors that contribute to bank fraud, including undertrained workers, insufficient managerial or supervisory oversight, and external influences. The study also discovered that frauds are challenging to prosecute because of challenging legal and judicial processes. **Dr. S. Venkata Ramana & Dr. S Gopi Krishna**[7]**,** concluded that the banking institutions should adapt their business models to reflect legal and technological changes and continuously assess their vulnerability to fraud and the methods they use to counteract it. **Parisha Singh**[8] concluded that the banking institutions should take the initiative to inform customers about potential risks to their money while using online banking and also numerous adjustments must be made to the current regulatory mechanism sinceit is ineffective and unable to fulfill the objective of reducing online fraud. **Dr. Madan Lal Bhasin**[9] in his paper revealed that ineffective employee training programmes, weak internal controls, and a lack of administrative oversight were the most frequent causes of non- compliance. Lastly, it was recommended that banks should use cutting-edge technologies like data mining techniques and forensic data analysis to combat the emergence of sophisticatedfraud techniques**. Divya K**[10] specifically mentioned the regulatory framework that is in place in India. It also highlighted emerging developments in Internet banking that handle cyber concerns, their advantages and cons. At the end, the researcher concludes that the current legal framework is unable to address the issue of consumer security due to ambiguity, which is a major problem in

[5] Usman Kabir Shah & Mahmood Hussain Shah, *Critical Success factors for preventing E-banking fraud*, 18(2) Journal of Economic Banking and Commerce, 1-14 (2014), https://www.researchgate.net/publication/285956803_Critical_success_factors_for_preventing_EBanking_fraud
[6] Sukanya Kundu & Nagaraja Rao, *Reasons of Banking Fraud – A Case of Indian Public Sector Banks*, 4(1) IJISMRD, 11 (2014), http://www.tjprc.org/publishpapers/2-39-1403249767-Information%20systems%20-%20IJISMRD%20%20-%20Reasons%20of%20banking%20fraud%20%20-%20%20%20Sukanya%20Kandu.pdf
[7] Dr. S. Venkata Ramana & Dr. S Gopi Krishna, *A study on impact of fraud in Indian Banking Sector (with special reference on retail banking product)*, 2 (6) INT'l J. of Academic Research and Development, 15 (2017), http://www.academicjournal.in/archives/2017/vol2/issue6/2-6-250.
[8] Parisha Singh, *Online Banking Frauds and Role of Government to Curb It: With Special Reference to India*, 3 SUPREMO AMICUS 365 (2018).
[9] Dr. Madan Lal Bhasin, *Menace of Frauds in the Indian Banking Industry: An Empirical Study*, 4(12) AJBMR, 1 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676466.
[10] Divya K, *Legal Aspects of Internet Banking in India*, 2(4) INT'l J.L. & MGMT. (2019), https://www.ijlmh.com/wp-content/uploads/2019/10/Legal-Aspects-of-Internet-Banking-in-India.pdf

 ISSN: 2582-6433

e-banking services. **Ayush Goel**[11] made the suggestion in the article that there should be proper monitoring of the banks to see if they are maintaining all the data properly and securely, and that the governing bodies should also laid down some new guidelines related to E-Banking, which would give both consumers and bankers some clarity. **Nilaya Murthy & Santosh Gopalkrishnan**[12] aims to understand whether there is a pattern or a sequence to digital frauds and whether a person's level of openness on social media has any bearing on whether they become victims of digital fraud in their paper. The paper depicted that the openness element has an impact on vulnerability as well as the threat and legal aspects of a propensity for digital fraud.

[11] Ayush Goel, *Overview on E-Banking in Indian Jurisdiction*, 3 INT'l J.L. MGMT. & HUMAN. 1589 (2020).
[12] Nilaya Murthy & Santosh Gopalkrishnan, *Does openness increase vulnerability to digital frauds? Observing social media digital footprints to analyse risk and legal factors for banks*, 64(4) INT'l J.L. & MGMT., 368 (2022), https://www.emerald.com/insight/1754-243X.htm

 ISSN: 2582-6433

E-Banking in India

Development of E-Banking in India

E-Banking, an internet-based system that is quick, affordable, and conveniently available for users to use from almost anywhere, has displaced traditional banking. India ranks as one of the top nations around the globe where the banking system has undergone a digital revolution, particularly since the demonetization in 2016.[13] To better serve their consumers, nowadays most banks improved or added internet banking facilities via internet or mobile applications.

Simply put, E-banking, "*also commonly known as net banking or online banking, is a technology that allows clients and banks to execute or supply monetary or non-financial services that were previously only possible in branch network by using internet".*[14] By signing up for Internet Banking with their bank, a person can perform a variety of tasks, including money transfers, bill payments, viewing bank balances, making fixed deposits, purchasing insurance policies, and more. E-banking is far more than a way to do financial business online. It also includes a numberof different categories, including CBS, mobile banking, numerous card kinds (debit, credit, prepaid, forex, travel, etc.), digital wallets, ATM banking, EFT, and ECS, to mention just some.[15]

The digitization of banking services has significantly improved banks' ability to handle high numbers of transfers and has gradually substituted money transfers. In order to handle requests and provide services to numerous consumers simultaneously, a variety of software programs and data transmission systems have been created. These systems give consumers a safe place where they can carry out their transactions by utilizing one-time passwords (OTPs), unique pass codes, and customer identification.[16]

Whereas conventional banking needed consumers to consult their local bank and carry out their transactions through that division alone, E-Banking, by connecting all of a bank's branch offices, delivers for an interconnected solution in which all services, such as transferring finances, trying

[13] PARISHA, *supra* note 2, at 365.
[14] *Id*
[15] *Id.*
[16]MADAN, *supra* note 9, at 3.

 ISSN: 2582-6433

to check bank balances, bank records, seeking cheque books, reserving fixed deposits, removing or depositing cash, etc., can be obtained from every branch or via Internet/Mobile payment systems.[17]

The automation has helped banks improve bank inter-connectivity and connections as well as inter-bank interactions, in addition to enhancing activities for the banks' consumers. In order to provide 24x7 internet banking services, gain more customers at low operating costs, reduce inconsistencies and forgery in inter/intra bank money transfers, and speed up correspondence among banking institutions and their branch offices, the RBI established a variety of communications networks, including BANKNET[18], RBINet[19] (which works over BANKNET), and INFINET[20]. These mechanisms have strengthened the incorporation of emerging technologies in the banking and financial industry.

E-banking had virtually eliminated the need for conventional bank, forcing banking firms to alter their business strategies and provide just about all online banking through internet gateways. Numerous Fintech Startup have been established over the past ten years in addition to Banks and Financial Organizations. These startups have taken over the financial industry, particularly in the fields of peer-to-peer borrowing, fund raising, insurance, payments aggregators and gateways, wealth management, etc.[21] In order to offer banking facilities with these digital apps, banks are working with all these Fintech startups.[22]

When it comes to digital banking systems and technologies in India, such as MICR, Electronic Clearing Service (ECS), RTGS, and NEFT, RBI has been the market leader. With banks

[17] MADAN, *supra* note 9, at 3.
[18] BANKNET is a packet switched X.25 based network, which user banks access through leased lines at the respective local centers using asynchronous ports on PADs and PC/UNIX machines with Computerized Message Transfer and File Transfer software. It provides various message formats for inter and intra-bank communications in respect of fund transfer applications, Bank transfer on own account, Bank transfer in favour of third party. It also facilitates critical data transmission and reporting of daily, weekly, monthly balances of Government accounts, foreign exchange rates etc.
[19] RBINet, is a communication software, which allows free format messaging and file transfer on the existing BANKNET infrastructure with the help of UNIX servers with enhanced security features such as end-to-end encryption, audit trail, etc.
[20] INFINET is a communication backbone in the form of a satellite network based on VSAT technology that was developed by Institute for Development and Research in Banking Technology (IDRBT) (set up by the Reserve Bank of India). The main objective of developing the network was to upgrade the existing systems and enhance their productivity and efficiency and facilitate internet banking.
[21] Bank for International Settlements (2019), Annual Economic Report', June
[22] DIVYA, *supra* note 10.

 ISSN: 2582-6433

supplying the primary activities for the payment services, RBI, as the controller of the financial markets, has not just built but also overseen and controlled the online transaction network. The notion that RBI Digital Payment Index (RBI-DPI) (with March 2018 as the benchmark)[23] stood at 270.59 in March 2021 as opposed to 100 in March 2018 provides evidence of the swift uptake and integration of digital payment platforms in India.[24]

After financial liberalization, numerous panels have been established by the RBI to include digital service delivery in the banking system of India.[25] The sudden increase of IT and IT- enabled operations has altered the financial sector worldwide. The objective of these panels was to define and coordinate financial technology across the Indian banking system. The digitization of banking services, which started with ATMs and credit/debit cards, has advanced to include payment gateways, aggregators, online banking, and mobile banking. But when it pertains to digital transactions, data privacy, and data security, there aren't many explicit, specific legislation, regulations, and restrictions.

Technology and the banking and finance industry's adoption of it present challenges and opportunities. Although it boosts productivity, the rising IT interdependence among banks, fintech startups, as well as other suppliers of financial IT solutions also raises the possibility of heightened cyber dangers. The complexity of the monetary institutions and the associated IT risks are increasing significantly, especially given that the majority of bank workers have little experience managing sophisticated IT systems. Although these technologies offer affordable services and improve access to financial services by making banking services available to the financially excluded sector, they also present administrative and regulatory challenges and significantly raise cyber security threats, particularly fraud risks.

E-Banking Frauds

The conventional approaches of bank fraud have been supplanted by E-Banking scams as a result of the rise of E-Banking, especially the transaction methods. Cybercriminals have taken advantage of E-Banking's flaws to break into banking institutions and fulfil their goals of making quick money with little danger of legal repercussions.

[23] https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR59740E2B9C4C4AA4EB5B8CD2AAAA670F19A
[24] Payment Systems in India – Booklet. https://m.rbi.org.in/scripts/PublicationsView.aspx?Id=20315#AP2
[25] DIVYA, *supra* note 10.

 ISSN: 2582-6433

Recent developments, such as the global pandemic brought on by the COVID 19 virus, have highlighted the expanding demand for and significance of E-Banking platforms. However, it also led to a rise in cyber-fraud instances.

Here are some of the e-banking frauds that have been covered.

Hacking

The most popular technique used by frauds to get unlawful entry to E services is to hack into systems via computer software that are especially made to look for gaps in the safety of the network and give the hacker' accessibility to the data contained there.[26] These details are used byfraudsters to carry out a variety of frauds, including unlawful financial transactions and digital purchases of products and activities using credit payment or bank account credentials.

Hackers utilize a variety of methods, including the use of malware, spyware, and computer viruses, key logger, adware, Trojan horse etc. to obtain data.

Phishing

Phishing is a type of scam that was noted as a security problem in the Working Group on Electronic Banking Report.[27] Phishing is the practise of asking recipients of emails to gain entry to one's login credentials, such as username and password, or other personal information, in to gain access to their profiles, even though the emails actually appear to have been sent by a trustworthy source, such as a bank or bank executive.[28] The explanations stated could be anything from the need for normal security checks to the need to verify the customer's information before transferring money. In order to fulfill these requirements, the email typically includes a link that takes the recipient to a bogus bank website. Once the recipient enters their credentials, the fraud has control of their financial accounts, checking accounts, as well as other internet banking accounts.

[26] DIVYA, *supra* note 10.
[27] Reserve Bank of India. 2011. *Report of The Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. Mumbai: Reserve Bank of India,* 59-61. accessed November 10, 2022, https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf
[28] PARISHA, *supra* note 2, at 365.

 ISSN: 2582-6433

For example, the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) held in the case of *IDBI Bank v. Sudhir S. Dhupia*[29], that in cases of phishing scams, where the banking institutions were guilty of negligence and their net banking institutions were not protected, they would be liable under Section 43(j), Section 43-A read with Section 85 of the ITA, 2000.

Vishing

Vishing, also known as voice phishing, is a kind of fraud that utilises Voice Over Internet Protocol (VoIP)[30] and social engineering techniques to obtain an user's financial data, including their card number, expiration date, Card Verification Value (CVV) number, one-time password (OTP), and bank account data.[31] The unexpecting consumers are called by con artists posing as bank officials in order to confirm their account information and convince them to reveal their private or economic information. Vishing scams typically try to collect credit card numbers or private information for use in identity theft and other illicit acts.

Card Skimming

Card skimming is a type of e-banking scam in which criminals attach a tiny gadget to an ATM card machine or other point-of-sale equipment in order to duplicate the data on a card which is swiped through the device. Card skimming devices read information from the magnetic stripe of the card, including the card number, expiration date, name of the cardholder, and CVV number. The gadget gathers data until the fraud removes it. The fraud may then employ the stolen information to either copy cards or use it for online transactions, often known as "card not present" scams. Scam artists also set up cameras or keyloggers to record the PIN of card users in conjunction to such card skimming equipment. Fraudsters may also employ this data to open an account or even request loans using the data of cardholders, in addition to utilizing it to copy cards.

[29] 2019 SCC OnLine TDSAT 226
[30] Voice over Internet Protocol (VoIP) is a technology that enables a user to make voice calls using the internet instead of regular telephone connections.
[31] DIVYA, *supra* note 10.

 ISSN: 2582-6433

Insider Risks in E-Banking

The benefit of their knowledge with and access to the frameworks which provide E-Banking Services and/or the centralized data centres combined with their access privileges to get around any safety precautions through legal channels makes an employee (current or former), third - party companies, and other insiders constitute a serious potential for fraud.[32]

Several academics interpret insiders as *"individuals, who are or were, permitted to access the systems and use the information held within these system' databases to carry out the job."*[33] Since insider fraud is frequently not disclosed by corporations out of concern regarding brand damage, it is hard to ascertain. Scholars have classified insider frauds as – *"Occupational White- Collar Crimes, which comprise legal infractions committed by an individual(s) while engaged in employment for illegal benefit".*[34] In other ways, occupational white-collar crimes include - *"when employees utilise their status inside a company to perpetrate certain illegal charge, utilizing their specific expertise of or accessibility to the firm's equipment".*[35]

The ACFE's 2004 Report on Occupational Fraud and Abuse, termed it as — *"the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."*[36] The Report states that occupational fraud refers to a variety of offences committed by staff at all levels inside a business, including robbery of office equipment, misappropriation, falsification of accounting results, money laundering, and theft of data. The Report also notes that there exist four key components to every occupational fraud, including (a) surreptitious action, (b) breaching the offender's legal responsibilities to the victim organization, (c) committing the conduct for the offender's direct or indirect economic gain, as well as (d) resulting the organization to lose investments, income, or deposits.[37]

[32] M.R Randazzo., et al, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* 2 Software Engineering Institute, Carnegie Mellon University (2005) https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14420.pdf
[33] PARISHA, *supra* note 2, at 368.
[34] *Id.*
[35] *Id.*
[36] Association of Certified Fraud Examiners, *Report to the Nation on Occupational Fraud and Abuse* https://www.acfe.com/uploadedfiles/acfe_website/content/documents/2004rttn.pdf
[37] Id.

 ISSN: 2582-6433

The ACFE examined 2,504 specific instances of employee fraud in 23 enterprises across 125 countries for its most recent Report of the Year 2021[38], and it discovered that the Banking and Financial Services Industry continued to occupy the top the spot with 386 cases that resulted in a mean average Damage of $100,000 in the year 2018–19.[39] These Reports show that, in comparison to other Industries, Banking and Financial Institutions are always more vulnerable tointernal fraud.

Insider Risks come from more than just intentional behaviour; carelessness or undertrained staff could play a role in the execution of frauds. Grossly negligent personnel put their companies at risk by failing to adhere to established procedures, resulting in data leaks, or accidentally installing malware, exposing back doors, etc. that fraudsters can use to their advantage. The rapidrate of technological advancement frequently necessitates the exporting of IT-related operations to outside suppliers. As a consequence, there is a lack of control and awareness over the networks that are utilised to provide the services and data needed by those operations, and several potential entry points into the E-Banking infrastructure are created. By using this weakness, workers and outside providers run the additional danger of engaging in fraud and erasing any potential evidence of their actions. Insiders have the best opportunity with the least chance of being caught or facing legal repercussions because banks are prime targets for fraudsters trying to make quick gains as money storage facilities. They have many chances and incentive because of their understanding of the networks and accessibility to them, particularly inE-Banking.

In India, the banking sector has expanded dramatically over the past ten years, with electronic banking now outpacing traditional banking. Extensive hiring, particularly at entry-level positions with no expertise, was required because of the growth which has considerably increased the chances of insider trading. The very innovation that has driven this expansion also creates an internal danger due to a lack of knowledge between older and younger staff. The supervisor or manager's insufficient technology expertise could result in a loss of command and give the employee a chance to perpetrate frauds undetected.

[38] Association of Certified Fraud Examiners, *Report to The Nations: 2020 Global Study on Occupational Fraud and Abuse (2020)* https://acfepublic.s3-us-west2.amazonaws.com/2020-Report-to-the-Nations.pdf.
[39] Association of Certified Fraud Examiners (ACFE), *Report to The Nations: 2018 Global Study on Occupational Fraud and Abuse* (2018), https://www.acfe.com/report-to-the-nations/2018/default.aspx

 ISSN: 2582-6433

Different platforms and technology are utilised by the numerous applications that banks use to offer e-banking services, such as CBS, ATM networks, internet and mobile banking, phone banking, EFT systems, and e-wallets, among others.[40] To ensure that the programs run well, those apps and technologies need personnel like workers, business associates, third-party contractors, and IT experts. Additionally, these applications execute a large volume of customer request and payments around-the-clock. Together, these factors make it challenging to adequately manage areas of access, leaving E-Banking open to ongoing security risks. In addition to regulation and legal difficulties, the difficulty of these systems also results in gaps such insiders having data access outside the authorised privileges, back doors, numerous permissions, or competing restrictions.

All organizations are affected by insider fraud; however, the damage done to banking and financial institutions is much more severe because it goes beyond just the immediate economic losses brought on by the frauds to include reputation damage failures that have an influence not just on the banks' capacity to keep customers but additionally on the whole banking system.[41]

The biggest fraud vulnerabilities coming from internal factors or insiders include everything from manipulating or abusing private and financial data to falsifying books and account balances, making unauthorized money transfer, approving credit and loans without proper verification, and attempting to steal information and details for espionage or personal profit.[42]

The following section discusses a few of the risks connected to insiders.

Theft from Account of Consumer's

Of the most frequent dangers in banking services, that has escalated with implementation of E-Banking, is insider theft from the account of a consumer[43] Because of extensive access credentials and system knowledge, bank workers have the capability to steal modest amounts outof a wide number of users and shift stolen funds to their personal account, the bank account of their acquaintances and relatives, or both. This kind of "*skimming"* is typically a long-winded

[40] MADAN, *supra* note 9, at 3
[41] *Id*
[42] ASHU & BINDU, *supra* note 4, at 5.
[43] *Id.*

 ISSN: 2582-6433

technique that is difficult to uncover because the exact figure is typically quite modest and therefore is frequently overlooked by the bank customers.

It is often referred to as *"salami slicing"* since the scammers take extremely little sums out of many accounts throughout the bank's whole infrastructure, but overall profits are enormous.[44]

Further techniques employed by the scammers include reversing bank fees and transferring the refunds into their personal account, as well as failing to report deposit operations in the customers' accounts on the database and withdrawing the funds for their own purposes. Similar to this, a bank employee or insider who is familiar with the system and how it operates can abuseand embezzle from funds that have been inactive or are laying idle.

Identity Theft

Among the perils of using online banking is identity theft, which helps criminals carry out their crimes. Since multiple levels of personnel require access to the information to perform daily tasks including transactions authorization, management of the CBS network, as well as other services used in E-Banking, the danger of identity theft by insiders is clearly reflected in the banking sector.[45] Inadequate permissions and privilege misuse are the main causes of insider fraud in banking and financial institutions. Considering the nature of e-banking, it is essential for employees, such as managers, transaction authorizers, and IT specialists, to have top level access permissions to the systems in order to carry out their responsibilities.[46] This gives them justification for accessing, adding, or changing data that is kept in those frameworks.

Often permissions provided for particular tasks are left in place after the work has been completed, allowing the normally uninvited individual or individuals extended accessibility and the chance to steal the data or influence the system for their own advantage with little chance of being discovered. This could be the result of IT staff members' negligence or a planned action to engage in illegal transactions in coordination with other bank staff. In October 2020, a reputable

[44] ASHU & BINDU, *supra* note 4, at 5.
[45] Id.
[46] Id.

 ISSN: 2582-6433

media reported on the capture of a banker perpetrating fraud by using identity theft.[47] The offender was employed as a representative of customer service in one of the Chennai-area officesof a banking company. The offender's method involves setting a bank account in some other bank using a phone he discovered on the side of the street and the identity of some other individual. In addition to creating a current account, he requested a merchant point of sale systemfrom the bank, claiming it was necessary for his company. He then persuaded the individual whose identity he had used to finish his KYC verification via video conference, citing the limits imposed as justification. When everything was ready, he approached a bank employee who already had a credit card customer and convinced them to fill out an application for credit card. The culprit then acquired the card's information and utilized a point-of-sale device to charge Rs.
10.36 lakhs to the card.[48] The consumer whom name the card had really been assigned received the bill and discovered he had already been taken advantage about when he went to the bank. The worker was implicated after a police report resulted to an inquiry.

This is only one instance of a bank employee using his role to steal someone else's information in order to commit fraud. Several similar occurrences have been documented worldwide, not just in India.

Data Theft

To fulfill consumers' service and operational requirements, e-banking services and systems maintain and process a substantial chunk of their financial and private data.[49] Due to the entire digitization of banking and the implementation of CBS, banks now keep vast quantities of financial and personal data about their clients, including identity, address, mobile phone number,Aadhar and PAN information, credit card information, passwords, and PINs.[50] This information, which clients give banks in order to use a variety of online banking, is a precious resource that is vulnerable to threats from both internal and external sources. Insiders pose a major concern because of their rights of accessibility to the systems that keep this information.

[47]R Sivaraman, *Bank executive held for identity theft, novel fraud* (2020) https://www.thehindu.com/news/cities/chennai/bank-executive-held-for-identity-theft novelfraud/article32808065.ece
[48] Id.
[49] ASHU & BINDU, *supra* note 4, at 5
[50] Id.

 ISSN: 2582-6433

Carelessness of the employees or deliberate behavior could lead to information breaches. In both situations, the outcomes could be significant in terms of reputational risk and lost income through suspicious transactions. Despite running the danger of being caught, a careless worker could depart his workstation without signing out, providing somebody employee the chance to enter the network outside his scope of authority and taking data for their own benefit. Employeesmay steal data for a variety of purposes, including spying, exploiting it for their own personal gain, offering it to other scammers for money, etc.

Herve Falciani's theft of client private details while employed by HSBC Bank as an IT Analyst is one of the most talked-about incidents illustrating the insider risk associated with data vulnerability.[51] The staffer in this instance stated that he took the information to expose the service's flaws, but the bank insisted that sabotage was the true motive.

Despite the fact that banks have several measures in place to guard against data theft, the characteristics of electronic banking services and the requirement to grant staff access rights to the data make insiders the greatest danger to defrauding by obtaining consumer information. The IT Act, 2000 also included penalties for data theft or unauthorised use, however it can be challenging to demonstrate when insiders with valid access to the information are involved.

Trading Fraud

Modern banking now offers services including financial services and investing in the securities markets, going well beyond the traditional roles of banks. There have been numerous instances where bank workers have allegedly engaged in illicit trading, causing the banks to suffer substantial losses. For illustration, one employee's illicit trading activities and abuse of his status and understanding of the bank's operations to conceal his liabilities in the securities market areto blame for the bankruptcy of Barings Bank.[52]

Insiders use money from bankers' suspense accounts to cover up deficits that may well have suffered on client savings and investments, present the accounts' balances to the clients as

[51] Hindustan Times. *HSBC whistleblower gets 5 years in jail for data theft, espionage (2015)*, https://www.hindustantimes.com/business/hsbc-whistleblower-falciani-gets-5- years-in-jail-for-data-theft-espionage/story-7eLjaoz7yNnS4Q0xilABcL.html.

[52] Ian Greener, *Nick Leeson and the Collapse of Barings Bank: Socio-Technical Networks and the 'Rogue Trader*, 13(3) SAGE PUBLICATIONS 421, 424 (2006), https://www.researchgate.net/publication/247747438_Nick_Leeson_and_the_Collapse_of_Barings_Bank_Socio - Technical_Networks_and_the_'Rogue_Trader'.

 ISSN: 2582-6433

favorable, and cheat them. After displaying the portfolios balances to the clients, the money are moved back to the suspense accounts.[53] By fabricating false bank records in the investment portfolios of the clients, dishonest insiders deposit the clients' funds in their own accounts and siphon off the profits.

Money Laundering

Due to their role as a conduit for banking transactions, banks run a very significant risk of someone being utilised for financial fraud. According to regulatory and supervisory challenges in compliance with Money Laundering rules, e-banking has heightened this danger even further. The creation of accounts using invented identities or fake KYCs that may be used to launder money, the approval of cash payments, and the processing of payments for financial profit are allreadily and deliberately done by bank workers.

E-banking systems can be utilized to engage in fictitious businesses, and fraud international transfers may be authorised based on deceptive import bills sent to unreachable firms. The majority of the time bank personnel who are knowledgeable of the fraudulent assist or collaborate with it. The majority of the time, bank staff assists or collaborate in such dishonest operations since they are conscious of the safety precautions that might otherwise set off electronic alarms and are capable of working around them.[54]

The use of e-banking services has made it harder to identify and prevent financial fraud because the information and transaction traces are frequently hard to follow when a large variety of transactions are conducted quickly. The problems are made worse by the malevolent Insiders' direct assistance of the offenders.

Circumventing Internal Controls

Banking laws and regulations, which serve as the initial line of protection against internal fraud and require experienced employees or even other coworkers to validate transactions beyond a specific threshold, too are subject to exploitation.[55] They can be readily avoided by an interior scammer by collaborating with coworkers or by utilizing the verifying veteran's passwords that

[53] Id.
[54] AYUSH, *supra* note 11, at 1589.
[55] AYUSH, *supra* note 11, at 1589

 ISSN: 2582-6433

the frauds may have obtained. The insider fraudster can confirm some suspicious transactions and escape detection by logging in with these passwords.[56] Additionally, insiders can restrict transfers underneath the second layer of verification by using their understanding of the bank's regulations regarding operations necessitating it.

In the overwhelming majority of cases of internal fraud, banks are hesitant to disclose them out of concern for reputational harm and choose to handle them privately, according to various studies on internal misuse and forgery. Internal frauds are frequently underreported, and by the time they are discovered, the offenders may have already departed the company or covered up any evidence that may point to them. Because there isn't enough evidence to punish the offenders, they have a chance to conduct the very same scams in some other bank.

Loan/Credit Fraud

Every bank's primary line of operation is lending, which is similarly prone to fraud from outside, inside, and coercive both internal and external causes. In the last ten years, banks have reported the most frauds in their loan and credit holdings.

Insiders approve loan requests and lines of credit without sufficient scrutiny or paperwork for individuals, their acquaintances, relatives, or even strangers for self benefit by using their official stance plus understanding of internal systems.[57] Numerous times, the debtors default on the loans, creating NPAs, and the absence of sufficient paperwork or scrutiny prior to approval makes recovery challenging or impossible.[58]

Account holders' personal identity data is also accessible to insiders, and there is a chance that dishonest insiders could have used such data to apply for loans or other lines of credit that usethe customer contact information or in the account numbers. Additional risk that insiders pose is the exploitation of loan accounts, including the removal of fees or modifying borrowing costs for personal advantage. Often these banks have internal rules, such as different staff for legitimizing or validating application forms, to decrease the incidences of insider scam; however, worker

[56] Rupa Rege Nitsure, *E-banking: Challenges and Opportunities*, 38 EPW, 5377 (2003), https://www.jstor.org/stable/4414436
[57] Id.
[58] Id.

 ISSN: 2582-6433

collaboration or trying to steal a colleague's qualifications for verification are danger that are challenging to manage and frequently impossible to spot.[59]

Like other businesses, banks have always been exposed to internal fraud threats. However, because of the variety of systems linked and their intricacy, E-Banking has highlighted these vulnerabilities.

Legislative Framework Combating Insider Risks

The dynamic nature as well as tactics of e-banking frauds had made them a burden for lawmakers. The RBI has established numerous committees and organizational units to examine

[59] Rupa Rege Nitsure, *E-banking: Challenges and Opportunities*, 38 EPW, 5377 (2003), https://www.jstor.org/stable/4414436

 ISSN: 2582-6433

the critical elements and vulnerabilities that fraudsters target, make recommendations for ways to secure the networks, and lay out strategies for lowering the amount of scams that are executed.

There is no specific law in India that defines frauds in the banking system as a specific crime. As a result, there are currently no explicit laws addressing insider fraud. A portion of the process for recognizing as well as fighting against fraud concerning bank personnel is covered mostly by Master Directions on Frauds-Classification and Reporting by Commercial Banks and select FIs, provided by the RBI.[60]

In accordance with the provisions of the aforementioned Master Directions, banks are obliged to reveal frauds of Rs 1 lakh or more to its board members and to present a Fraud Monitoring Return (FMR) to the RBI within three weeks of the fraud's discovery.[61] The measures taken by the investigating branch against the fraud-committing workers should also be included in the presentation to the Board. In accordance with these Master Directions, the Regional Head of the Bank must be notified of any fraud involving bank staff that is less than Rs 10,000.[62] The Master Directions specify whenever and to what agency banks must disclose any instances of fraud in order to guarantee that the offenders are held accountable.

The Companies Act of 2013, the PCA of 1988, the PMLA of 2000, the Whistleblower Act of 2014, the Consumer Protection Act of 2019, the RBI Circulars and Directions regarding Customer Protection and security of E-Banking Services, as well as other laws focus on providing additional strategies to counter the threat of insider frauds in addition to the aforementioned Master Directions.

The Companies Act, 2013

[60] RUPA, *supra* note 56, at 5380.
[61] Id.
[62] Id.

 ISSN: 2582-6433

The Private sector banks must abide by the terms of the Companies Act of 2013 since they are controlled by private companies or people, are registered under the Companies Act of 2013, and have been granted licenses underneath the Banking Regulation Act of 1949.

All businesses incorporated under Companies Act of 2013 are required to abide by a number of internal control regulations, including those pertaining to disclosure, auditing, monitoring mechanisms, and processes for risk management.[63] In addition to such, the Companies Act of 2013 defines fraud in respect to corporations and stipulates fines and sentences if the firm or its executives are charged with a criminal fraud.[64]

The following key clauses from The Companies Act of 2013 are important for dealing with the problem of insider risks:

- The creation of such an audit committee made up of autonomous plus executive directors is addressed in Section 177. The Audit Committee is in charge of, among many other things, making sure that both internal and external auditors' reports[65] are true and independent, evaluating inner financial reporting,[66] and establishing a framework for directors and managers to alert the Committee to any misgivings they might well have concerning any misconduct or deviations on the part of another worker.[67] The Audit Committee assures also that internal corporate controls are effective that don't provide dishonest people a chance to take advantage of their privileges and engage in fraud.
- In pursuance of Section 188, which addresses transactions between related parties every Contract or Agreement must first have special resolution consent from the firm. If a person is linked to a group to certain Contracts or Agreements, furthermore it restricts their ability to vote on these special resolutions. Only with intention of defrauding the organisation, this clause prevents boards and senior executives from abusing their positions for private profit.[68]

[63] Usman Kabir Shah & Mahmood Hussain Shah, *Critical Success factors for preventing E-banking fraud*, 18(2) Journal of Economic Banking and Commerce, 1-14 (2014), https://www.researchgate.net/publication/285956803_Critical_success_factors_for_preventing_EBanking_fraud
[64] *Id.*
[65] Section 177(4)(ii), Companies Act, 2013
[66] Section 177(4)(vii), Companies Act, 2013
[67] Section 177(9), Companies Act, 2013
[68] Sec. 188, Companies Act, 2013

 ISSN: 2582-6433

- Audit independence is a key component of any successful governance frameworks. The hiring of an Independent Auditor (or auditors) is required under Section 139. These individuals are mostly in charge of making sure that the corporation's financial records are kept in conformity with Accounting Standards and verifying that the accounting standard has not been manipulated or falsified.[69] This Section limits the period of employment to a maximum of ten years, significantly ensuring the autonomy and impartiality of the Auditors.[70] This protects the objectivity of the auditors, which in turn makes it easier to identify and stop fraud committed both by people and companies.
- Section 134 assures that Financial Statements and Board Reports, which cover every component of the company and governance of the corporate board, are disclosed properly.[71] It stipulates that Director's Report must contain a comment outlining the strategy for risk management and how it is being implemented, as well as any concerns that have recently been recognized and any steps taken to limit potential losses incurred as a result of such risks. Misleading statements in any audits, declarations, or other papers that must be provided in accordance with the 2013 Companies Act or its regulations are punishable under Section 448.[72]
- Section 447[73] specifies frauds in respect to businesses and especially outlines punishments for frauds. The term "fraud" in the context of this Section expressly refers toany form of deception perpetrated with the goal of deceiving by Insiders, either alone or in concert with anyone else, including any omissions, action, or misuse of authority. The differentiating characteristic of this concept is that it is irrelevant if there was any unjust profit or loss provided the motive to deceive is established.

[69] Section 143, Companies Act, 2013
[70] Section 139(2), Companies Act, 2013
[71] Sec. 134, Companies Act, 2013
[72] Sec. 448, Companies Act, 2013.
[73] Section 447: Punishment for fraud: Without prejudice to any liability including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud 1[involving an amount of at least ten lakh rupees or one per cent. of the turnover of the company, whichever is lower] shall be punishable with imprisonment for a term which shall not be less than six months, but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extendto three times the amount involved in the fraud: Provided that where the fraud in question involves public interest, the term of imprisonment shall not be less than three years. Provided further that where the fraud involves an amount less than ten lakh rupees or one per cent. of the turnover of the company, whichever is lower, and does not involve public interest, any person guilty of such fraud shall be punishable with imprisonment for a term which may extend to five years or with fine which may extend to fifty lakh rupees or with both.

 ISSN: 2582-6433

It is important to note that just Private Banks are subject to the Companies Act of 2013, leaving out those other financial organisations including Public Sector Banks, Foreign Banks, and Cooperative Banks. To solve these issues, the RBI gives guidance and recommendations on corporate governance on a regular basis, which all financial institutions must follow.

Prevention of Corruption Act (PCA), 1988

The PCA is a significant piece of law that's been passed with the intention of reducing public servant corruption. The PCA covers bribery, misappropriation, getting any financial benefit, owning property and assets out of relation to one's earnings, and abusing one's status and authority to offer the other an extra edge for personal profit, among other things.[74]

According to PCA, 1988, the definition *"public servant"* refers to all people who carry out public duties, including government workers as well as bank staff, university vice chancellors and professors, jurists and judicial officers, associates of any service commission board or selection committee, etc.[75] In addition to those who receive an unfair advantage, the PCA of 1988 also applies to those who promise or really provide an extra edge to a public servant.

Insider-committed bank fraud is typically the subject of allegations made underneath the PCA, 1988. A Special Court that has been explicitly formed under such a Act for expedited proceedings hears certain matters. When actually convicted, the penalties have included a penaltyas well as a least of three years to a maximum of seven prison term.[76]

The above clauses deal with the problem of insider frauds in part, but as is evident from the analysis of insider risks from the above, not all insider frauds would be covered by PCA, 1988.

Prevention of Money Laundering Act (PMLA), 2002

[74] USMAN & MAHMOOD, *supra* note 63, at 10.
[75] Section 2(c), Prevention of Corruption Act, 1988
[76] Section 7, Prevention of Corruption Act, 1988

 ISSN: 2582-6433

Under the PMLA, 2002, banking and financial firms are obliged to keep track of all transactions and client identity documents[77], particularly in situations of cash transactions or withdrawal of funds, deals involving foreign exchange above the permissible limits, large value imported goods or cash transfers, and every other high-risk money transfers[78], and to provide those documentation, inside the specified timeframe, to the Officials designated. Although these regulations don't directly address how to avoid bank fraud, they are useful for tracking down offenders and conducting investigations.

The proceeds of crime[79] are also defined in PMLA, 2002, along with scheduled offences[80] (that include IPC offences like cheating, forgery, etc.) and PCA, 1988. This gives the investigative authorities the authority to charge the perpetrators with violations of the PMLA, 2002, creating a deterrence impact.

Information Technology Act (ITA), 2000

The conventional manner of doing banking underwent a fundamental change as a consequenceof technical advancements, which forced both banking and financial products sector to change its business plan in order to offer speedier services at a lower cost. This came with their own risks and legal concerns in addition to the benefits of service exports and good services. The ITA, 2000 was implemented in India in order to address the issues presented on by the incursion of technology in all fields.

Electronic flow of funds among banks and other financial institutions the upkeep of Bankers Books in digital mode, the legal protections of online transactions, agreements reached via electronically exchanged information and other forms of online correspondence, digital

[77] Section 12, Prevention of Money Laundering Act, 2002
[78] Section 12AA, Prevention of Money Laundering Act, 2002
[79] Section 2 (u), ―proceeds of crime‖ means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property or where such property is taken or held outside the country, then the property equivalent in value held within the country or abroad. Explanation.—For the removal of doubts, it is hereby clarified that "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence;
[80] Section 2 (y) ―scheduled offence‖ means— (i) the offences specified under Part A of the Schedule; or (ii) the offences specified under Part B of the Schedule if the total value involved in such offences is 7 one crore rupees or more; or (iii) the offences specified under Part C of the Schedule.

 ISSN: 2582-6433

signatures and their verification, and punitive measures and sanctions for crimes perpetrated utilizing electronic media were all covered.

Sections 43 and 43A of the Information Technology Act of 2000 (ITA, 2000) provide penalties, damages, and consequences for fraud or dishonest acts that result in computer system damage, and Section 66 provides damages for failure to protect sensitive information assigned to any incorporated body.[81] According to Section 66C[82], identity theft is penalized by up to three years in prison and a penalty of up to Rs 1 lakh for anyone found guilty of using another user's electronic signature, passcode, or other distinguishing identification credentials deceitfully or illegally. According to Section 66D[83], the maximum sentence for impersonating someone else to commit fraud that used a computer is three years in jail with a heavy penalty of Rs. 1 lakh.

The Indian Computer Emergency Response Team would have been a governmental body for crisis response with its major purposes being accumulation, assessment, able to broadcast of dataof cyberattack, as well as issuing of rules and notices regarding cyber security. This would be established under Section 70B of the ITA, 2000.[84]

The researcher would also like to emphasize once more that whilst ITA, 2000 may indeed recognize online transactions legally and offers civil and criminal penalties for their violation, it is insufficient to address both the evolving business operations of banks and the evolving nature of the frauds committed here anyway.

Payment and Settlement Systems Act, 2007

The IT Act of 2000 was required by the advancement of technology, and the PSSA of 2007 was required by the emergence of Financial Technology, or Fintech, in the provision of bank services. It outlines the control and oversight of India's payment services, with the RBI acting as the designated supervisor.

[81] Information Technology Act, 2000, pg. 18
https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[82] IT Act, 2000.
[83] IT Act, 2000.
[84] Sec. 70 B, IT Act, 2000.

 ISSN: 2582-6433

The advent of numerous payment services like RTGS, NEFT, IMPS, as well as other Payment Gateways and Aggregators as a result of the financial integration and digitization of banks necessitated the creation of a legal foundation for their resolution. The PSSA, 2007, defines terms like *"Payment Obligation,"*[85] *"Settlement,"*[86] *"Netting,"*[87] and *"Payment System,"* [88] and Section 5 of the law gives RBI the authority to grant permission to any element wishing to launch or operate a Payment System if it complies with the criteria established by RBI for that reason.

Given that the majority of money transfers are now digital, the PSSA, 2007 not only allows for the regulation and monitoring of the multiple payment options that are presently accessible, but also gives the RBI significantly larger control over the activities of organizations apart from financial companies and banks that offer these services. Although this is crucial for operational stability, The PSSA, 2007 only addresses the problem of frauds committed via these Payment Systems or Gateways by stipulating that system participants are liable in the event of any "Systemic Risk".[89]

Overall summary, a number of laws have indeed been passed to oversee and govern the banking industry, yet none of them particularly tackle the problem of bank fraud. The most susceptible industries to fraud are banking and financial organizations and legislative change to combat bank fraud has typically been ex post facto or retrospective rather than active. Most laws addressing

[85] Section 2(1)(h) ―payment obligation means an indebtedness that is owned by one system participant to another system participant as a result of clearing or settlement of one or more payment instructions relating to funds, securities or foreign exchange or derivatives or other transactions.

[86] Section 2(1)(n) ―settlement means settlement of payment instructions and includes the settlement of securities, foreign exchange or derivatives or other transactions which involve payment obligation.

[87] Section 2(1) (e) ―netting means the determination by the system provider of the amount of money or securities, due or payable or deliverable, as a result of setting off or adjusting, the payment obligations or delivery obligations among the system participants, including the claims and obligations arising out of the termination by the system provider, on the insolvency or dissolution or winding up of any system participant or such other circumstances as the system provider may specify in its rules or regulations or bye-laws (by whatever name called), of the transactions admitted for settlement at a future date so that only a net claim be demanded or a net obligation be owned;

[88] Section 2(1) (i) ―payment system means a system that enables payment to be effected between a prayer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange. Explanation.- For the purposes of this clause, ―payment system‖ includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations

[89] Section 2(1)(o) ―systemic risk means the risk arising from— (i) the inability of a system participant to meet his payment obligations under the payment system as and when they become due; or (ii) any disruption in the system, which may cause other participants to fail to meet their obligations when due and is likely to have an impact on the stability of the system: Provided that if any doubt or difference arises as to whether a particular risk is likely to have an impact on the stability of the system, the decision of the Reserve Bank shall be final

 ISSN: 2582-6433

one type of bank fraud or another have been passed into law or changed as a result of numerous frauds.

Consumer Protection Act, 2019

Besides offering a venue toward which bankers can turn to enforce their rights in the event of a deficit in E-Banking Services, such as a violation of data protection and identification or other unlawful transactions, the Consumer Protection Act, 2019 safeguards the interests of bank clients.

In order to better safeguard consumer rights in the event of fraudulent transactions, the RBI issued directives[90] to all commercial banks restricting consumer responsibilities in the case of unlawful E-Banking transactions. In order to provide safety and privacy when conducting E- Banking activities with efficient measures of identifying and monitoring frauds, the directives require the enhancement of E-Banking process and practices.

The instructions also state that every fraud that happens as a result of carelessness, participation, or insufficiency on the portion of the bank, regardless irrespective of whether the consumer discloses the transfer of funds or not, as well as any fraud that happens as a result of external infringements in which neither the bank nor the consumer is at fault, must be reported by the consumer within three days after receiving notification from the bank of the illegal act.[91]

The consumer would be liable to no culpability,[92] and the bank would've been required to show that the consumer is responsible for the improper E-Banking activity.[93]

The RBI also frequently publishes Master Directions, Circulars, and Guidelines to Banks and Financial Institutions regarding the security requirements to be implemented in respect of all E-Banking Services, in addition to these pieces of legislation.

Even though E-Banking Services must adhere to strict security protocols, scams are expanding at an astonishing rate. The legislative and administrative features of e-banking as well as the safety

[90] Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions* (2017), https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15D620D2C4D2CA4A33AABC928CA6204B19.PDF
[91] Ibid Para 4 pg.2
[92] Ibid Para 6 pg.3
[93] Ibid Para 12 pg.6

 ISSN: 2582-6433

precautions that must be put in place to reduce the frequency of fraud utilizing e-banking services have been the focus of the committees as well as working bodies of the RBI.[94] The suggestions made by such Committees typically focus on enhancing internal and external controls as well as surveillance systems, but they do not clearly outline what disciplinary measures should be implemented to deter future offences.

[94] *Supra* note 90, at 6

 ISSN: 2582-6433

Conclusion and the way forward

The banking industry's customer service and business strategies have undergone a major transformation as a result of the introduction of technologies. In addition to greater customer support, access to financial services, and quicker, more affordable banking solutions, automation has also sparked worries about its serious contradictions, including fraud risk assessment.

Since its beginning, fraudsters have targeted the banking and financial industry as a sector. In contrast to techniques utilized in conventional bank, fresh avenues for frauds have become available thanks to the automation of banking services, as stated above, with fewer risks of being caught and punished and bigger benefits. Parallel to how external fraud threats have always existed in the banking industry, internal fraud potential have expanded as a result of the E- Banking industry's rapid rise. Internal frauds have increased owing to the intricacies of e- banking platforms, which use a variety of technologies and access credentials. With their detailed understanding of internal rules and user permissions, insiders present an equal if not larger threat of perpetrating frauds or collaborating with outsiders to aid the execution of frauds for personal gain.

Despite the fact that the banking and financial sector is one of the most heavily controlled and monitored, the emphasis of the these legislation and regulatory requirements is more on creating a financially stable system and ensuring that there are sufficient safeguards in place to reduce operations and maintenance exposures brought on by the risks related to dealing in financial assets. The legislation does not typically follow fraud risk, which makes it challenging to resolvethe problem. This is made much more obvious in the instance of internal frauds since, in additionto the absence of regulation, banks are reluctant to disclose instances of internal fraud to the regulators.

Additionally, frauds may harm the legitimacy and security of the economy as well as have a crippling impact on consumer trust in the banking sector. It may collapse banks and jeopardise RBI's oversight responsibilities. In summary, the researcher discovers that although financial and banking frauds receive a significant amount of public and press exposure, they take a decadeto uncover and establish. A large part of what motivates others to conduct frauds is the low probability of criminal identification and prosecution. This field is incredibly understudied and

 ISSN: 2582-6433

uncontrolled due to the lack of a complete law that recognizes and addresses bank fraud as a distinct category of financial crimes.

According to the analysis, bank fraud is one of the elements of economic crimes and it is not clearly covered by either the legislation or the government. The governance structures areessential for the prevention of financial crimes, especially when insiders are involved in bank fraud.[95] While the researcher concurs that not every forms of insider fraud can be totally stopped or minimized, however stronger legal as well as internal controls can halt the bulk of fraudulent acts.

The suggestions are broken down into two parts based on the research's conclusions, with the first heading dealing with legislative measures and the second with internal measures.

Legislative measures

- It is advised that a distinct law be passed to address financial frauds in the banking and financial sector. This legislation should make financial frauds illegal in order to effectively dissuade anybody from engaging in or attempting to engage in these kind of fraudulent acts. In addition to defining fraudulent transactions, the legislation should outline the procedures for a special independent investigating agency, special courts or tribunals, and punishment of such crimes. The investigating system needs personnel with expertise in finance and law, as well as modern technology instruments for early fraud detection and the ability to conduct efficient investigations on schedule. The judges or presiding officials of the Special Courts or Tribunals should ensure that prosecutions for such crimes proceed quickly, and they should be knowledgeable in both statutory and administrative standards as well as economic and financial structures. As a result, incidents involving financial fraud in banks would be promptly detected, punished, and the offenders would not escape penalty.
- To properly listen to the concerns of data and identity fraud, it is necessary to adopt privacy regulations that impose duty and accountability on those charged with consumers' personal and financial data.

[95] *Supra* note 90, at 6.

 ISSN: 2582-6433

- Being the supervisor, RBI is only permitted to conduct disciplinary procedures against the Regulated Entities and is not permitted to make fraudulent practices illegal. To safeguard the welfare of the wider populace, it is advised that RBI take stringent measures against such Regulated Entities where substantial value frauds have been discovered and revealed, including harsh punishments and potentially the termination of their licenses.

Internal measures

Even without assistance of internal factors, it is highly challenging for strangers to effectively commit fraud in instances of bank fraud. Therefore, it has been believed that internal controls are essential for preventing internal fraud. The research shows that internal frauds not only accountable for immediate cash damages but also for reputational harm, which results in a decline in sales and income. Corporate Governance models and well-maintained internal controls are crucial in giving remedies to internal fraud because laws alone are insufficient to reduce insider risks. Thus, it is advised that:

- With rigorous adherence to the Best Practices Code which the banks have produced for their workers and contractors, corporate governance in banks must be enhanced. The Best Practices Code shall specifically outline the obligations and expectations that bankers and third-party contractors must uphold with regard to online banking.
- The accessibility credentials for e-banking services must be rigorously checked and managed to prevent abuse. The password used to connect to the services must be changed frequently as a necessity. To avoid accidentally giving those who are no longer authorized access credentials, the access permissions should be reviewed routinely.
- Bankers must employ data forensics and technologies to identify questionable activity for early detection of fraud.
- Recognizing one's staff is just as crucial as recognizing one's clients. Many insider frauds can be avoided by routinely updating personnel identities and private details. Banks' human resource regulations must call for recurring exchanges with their workforce in order to learn more about their requirements, goals, and complaints. Any

 ISSN: 2582-6433

strange attitude that might be observed should be noted, and such individuals' conduct must be taken into consideration.

- The management or board has the flexibility to conduct an internal investigation or submit instances of insider abuse to team responsible under the existing framework of disclosing internal fraud, which creates vagueness. Any instance of internal fraud must beproperly probed by a special committee that the banks will appoint. The implicated should be suspended, and if crime is obvious or proven, swift legal action needs to be taken to dissuade everyone else from committing similar behavior.

 ISSN: 2582-6433

BIBLIOGRAPHY

Books:

- B.R SHARMA, BANK FRAUD: PREVENTION & DETECTION (Universal Law Publishing Co. Pvt. Ltd. 2009).
- R.P NAINTA, BANKING SYSTEM, FRAUDS AND LEGAL CONTROL (Deep & Deep Publication Pvt. Ltd. 2005).

Journals:

- Dr. S. Venkata Ramana & Dr. S Gopi Krishna, *A study on impact of fraud in Indian Banking Sector (with special reference on retail banking product)*, 2 (6) INT'l J. of Academic Research and Development, 15 (2017), http://www.academicjournal.in/archives/2017/vol2/issue6/2-6-250
- Parisha Singh, *Online Banking Frauds and Role of Government to Curb It: With Special Reference to India*, 3 SUPREMO AMICUS 365 (2018).
- Ashu Khanna & Bindu Arora, *A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry*, 4(3) INT'l J. of Business Science and Applied Management, 1 (2009), https://www.business-and-management.org/library/2009/4_3--1-21-Khanna,Arora.pdf.
- Usman Kabir Shah & Mahmood Hussain Shah, *Critical Success factors for preventing E-banking fraud*, 18(2) Journal of Economic Banking and Commerce, 1-14 (2014), https://www.researchgate.net/publication/285956803_Critical_success_factors_for_preventing_EBanking_fraud.
- Sukanya Kundu & Nagaraja Rao, *Reasons of Banking Fraud – A Case of Indian Public Sector Banks*, 4(1) IJISMRD, 11 (2014), http://www.tjprc.org/publishpapers/2-39-1403249767-Information%20systems%20- %20IJISMRD%20%20-%20Reasons%20of%20banking%20fraud%20%20-%20%20%20Sukanya%20Kandu.pdf
- Dr. Madan Lal Bhasin, *Menace of Frauds in the Indian Banking Industry: An Empirical Study*, 4(12) AJBMR, 1 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676466.

 ISSN: 2582-6433

- Divya K, *Legal Aspects of Internet Banking in India*, 2(4) INT'l J.L. & MGMT. (2019), https://www.ijlmh.com/wp-content/uploads/2019/10/Legal-Aspects-of-Internet-Banking-in-India.pdf
- Ayush Goel, *Overview on E-Banking in Indian Jurisdiction*, 3 INT'l J.L. MGMT. & HUMAN. 1589 (2020).
- Nilaya Murthy & Santosh Gopalkrishnan, *Does openness increase vulnerability to digital frauds? Observing social media digital footprints to analyse risk and legal factors for banks*, 64(4) INT'l J.L. & MGMT., 368 (2022), https://www.emerald.com/insight/1754-243X.htm
- M.R Randazzo., et al, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, 2 Software Engineering Institute, Carnegie Mellon University (2005) https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14420.pdf
- Ian Greener, *Nick Leeson and the Collapse of Barings Bank: Socio-Technical Networks and the 'Rogue Trader*, 13(3) SAGE PUBLICATIONS 421, 424 (2006), https://www.researchgate.net/publication/247747438_Nick_Leeson_and_the_Collapse_of_Barings_Bank_Socio -Technical_Networks_and_the_'Rogue_Trader'
- Rupa Rege Nitsure, *E-banking: Challenges and Opportunities*, 38 EPW, 5377 (2003), https://www.jstor.org/stable/4414436
- Dr. Sahila Chaudhry, Risk of Frauds in Indian Banks in E-banking Scenario, 8(5) Asia Pacific Journal of Research in Business Management, 8 (2017), https://www.academia.edu/33472938/RISK_OF_FRAUDS_IN_INDIAN_BANKS_IN_E_BANKING_SCENARIO.
- Mostafa A. Ali, Nazimah Hussin, Ibtihal A.Abed, E-banking Fraud Detection: A Short Review, 6(8) INT'l J. of Innovation, Creativity & Change, 67 (2019), https://www.ijicc.net/images/Vol6Iss8/6806_Ali_2019_E_R.pdf.
- Ainsey Granville, Andre Jorge Bernard, Brahma Edwina Baretto, Rodney D' Silva, Impact of Frauds on the Indian Banking Sector, 8(752) INT'l J. Innovative Technology & Exploring Engineering, 8 (2019), https://www.ijitee.org/wp-content/uploads/papers/v8i7s2/G10370587S219.pdf

 ISSN: 2582-6433

Websites/Webpage:

- Payment Systems in India – Booklet. https://m.rbi.org.in/scripts/PublicationsView.aspx?Id=20315#AP2
- Reserve Bank of India. 2011. *Report of The Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. Mumbai: Reserve Bank of India*, 59-61. accessed November 10, 2022, https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf
- Association of Certified Fraud Examiners, *Report to the Nation on Occupational Fraud and Abuse* https://www.acfe.com/uploadedfiles/acfe_website/content/documents/2004rttn.pdf
- Association of Certified Fraud Examiners, *Report to The Nations: 2020 Global Study on Occupational Fraud and Abuse (2020)* https://acfepublic.s3-us-west2.amazonaws.com/2020-Report-to-the-Nations.pdf
- Association of Certified Fraud Examiners (ACFE), *Report to The Nations: 2018 Global Study on Occupational Fraud and Abuse* (2018), https://www.acfe.com/report-to-the-nations/2018/default.aspx
- R Sivaraman, *Bank executive held for identity theft, novel fraud* (2020) https://www.thehindu.com/news/cities/chennai/bank-executive-held-for-identity-theft novelfraud/article32808065.ece
- Hindustan Times. *HSBC whistleblower gets 5 years in jail for data theft, espionage (2015)*, https://www.hindustantimes.com/business/hsbc-whistleblower-falciani-gets-5-years-in-jail-for-data-theft-espionage/story-7eLjaoz7yNnS4Q0xilABcL.html.
- Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions* (2017), https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15D620D2C4D2CA4A33AABC928CA6204B19.PDF

 ISSN: 2582-6433

Table of Abbreviations

ABBREVIATIONS	FULL FORM
ACFE	Association of Certified Fraud Examiners
ATM	Automated Teller Machine
CBS	Core Banking Solutions
CVV	Card Verification Value
ECS	Electronic Clearance Service
EFT	Electronic Funds Transfer
IT	Information Technology
KYC	Know Your Customer
NEFT	National Electronic Funds Transfer
OTP	One Time Password
PCA	Prevention of Corruption Act
PMLA	Prevention of Money-Laundering Act
RBI	Reserve Bank of India
VoIP	Voice Over Internet Protocol
TDSAT	Telecom Disputes Settlement and Appelllate Tribunal