

EVALUATION ON DIGITAL BANKING FRAUDS: A LEGISLATIVE FRAMEWORK

Subhashis Chakrabartty

Research Scholar
20114281232046

Law

Dr. Kishwar Parween

Supervisor

Seacom Skills University, West Bengal

DECLARATION: I AS AN AUTHOR OF THIS PAPER /ARTICLE, HERE BY DECLARE THAT THE PAPER SUBMITTED BY ME FOR PUBLICATION IN THE JOURNAL IS COMPLETELY MY OWN GENUINE PAPER. IF ANY ISSUE REGARDING COPYRIGHT/PATENT/OTHER REAL AUTHOR ARISES, THE PUBLISHER WILL NOT BE LEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENT FROM THE JOURNAL WEBSITE. FOR THE REASON OF CONTENT AMENDMENT /OR ANY TECHNICAL ISSUE WITH NO VISIBILITY ON WEBSITE /UPDATES, I HAVE RESUBMITTED THIS PAPER FOR THE PUBLICATION.FOR ANY PUBLICATION MATTERS OR ANY INFORMATION INTENTIONALLY HIDDEN BY ME OR OTHERWISE, I SHALL BE LEGALLY RESPONSIBLE. (COMPLETE DECLARATION OF THE AUTHOR AT THE LAST PAGE OF THIS PAPER/ARTICLE

Abstract:

E-Banking or digital banking is inevitable for development because it counters the challenges being confronted by conventional keeping money around the world and encouraging online transactions with the tap of a mouse. Speed and precision are the modern mantras of the E-Banking framework. Within the time of E-Banking, unused modes of exchanges like RTGS, NEFT, ECS and EFT has captured the spotlight encouraging national and worldwide exchanges. The problem has started manifolds in the banking sector which is a result of frauds being done by spammers and fraudsters from several corners of the world. In this article, evaluation on digital banking frauds: a legislative framework has been discussed.

Keywords: Digital, Banking, Frauds, Legislative, Framework.

INTRODUCTION:

The robbery of electronic personality of an individual is known as 'PHISHING' in fraudster's speech. It may be an exceedingly profitable business. [1] In USA alone the number of yearly personality robberies is around one crore. The Web has included to the measurements of the issue. Numerous an individual has been the casualty (ordinarily the shippers who offer products to the cheat of electronic character). [2] The casualties of the burglaries endure overwhelming misfortunes in cash, kind and notoriety. Over all, it demoralizes the client, the bank and the genuine

vendor a parcel. [3] The client is despondent in case his bank is incapable to secure his E-banking transactions. He is disappointed, on the off chance that he should go to the court to clear the mess made by the electronic personality burglary. [4] Thus, most of the banks avoid the unfavourable reputation and take the misfortunes as commerce risk costs. They don't go in for examination or case. [5]

METHODOLOGY:

Doctrinal research methodology was used for this research with extensive use. Tools like statutory materials, case reports, periodicals, government reports, national & international journals e-resources etc. were used. Secondary data sources and qualitative research design were also used for this study.

ANALYSIS, OBSERVATION, RESULTS AND DISCUSSION:

ATM Fraud:

The security of the Automated Teller Machines (ATM) through ATM cards has expanded colossally in later a long time in India and it is expanding. Measures by the banks have made the mode of payment of cash exceptionally well known. Be that as it may, the fraudster is additionally in interest to manhandle the ATMs.

ATM Card is like a charge card. All the fakes which are committed with a credit or charge card can be committed with an ATM card.

A number of times before, an ATM of a bank was set absent and outside the bank. The wires had to pass through space which may well be drawn closer by open. Two fraudsters were on the post for a helpful time. One day they found a client coming to the ATM at an odd hour. The fraudster put up an electronic gadget along the wires interfacing the ATM with the bank and recorded the signals made by the withdrawal handle. As before long as the client cleared out the ATM, one of the two went interior the ATM booth and the other replayed the recorded information. The ATM reacted and conveyed the cash to the fraudsters.

In a later case, a military work force utilized an ATM to pull back cash. He found that one of the 1000 rupee notes was mutilated. He was to some degree shocked as ATM ordinarily conveys new cash notes. He went to the bank owning the ATM. He was told that the note was a manufactured note. The bank was surprised. The bank was not beyond any doubt whether the client is taking them for a ride or the contract office which filled the notes within the ATMs has done the trap. But to maintain a strategic distance from antagonistic exposure they supplanted the manufactured money note.

The Finance Ministry has reported to a Parliamentary Committee that frauds reported for ATMs and others have seen over 65 per cent growth in 2022 from 2021, while amount involved has nearly doubled. At the same time, National Payment Corporation of India has informed that on an average, 2,000 customers are impacted every month due to cyber fraud.

NEFT Fraud:

The exchange of cash from one put to another, through electronic gadget is Electronic Finance Exchange (EFT). In India EFT is given the title NEFT (National Electronic Finance Exchange). RBI (Save Bank of India) ignores the exchanges. In any case, it includes more often than not high-value instalments. EFT (or NEFT) exchanges are not numerous numerically. Value-wise, be that as it may, they account for almost 85% of the money development. Each exchange is of tall esteem. Indeed a single extortion in EFT may cruel misfortune of crores of rupees. EFT is additionally called Wire Exchange.

Armand Moore was a con artist of Chicago and thought exceptionally tall of him within the profession'. His life fashion requested that he ought to be a multimillionaire in the event that not a extremely rich person. Whereas serving a four-year internment for a con craftsmanship work he came to know how millions may be cheated through application of con craftsmanship in EFT exchanges. He arranged the greatest heist to gather \$ 200 million when he was behind the bars!

Mr. Moore, on coming out of the jail, enroped a bank employee, Taylor. He was an representative of the most bank in Chicago (To begin with National Bank) and worked within the EFT department of the bank, along side another worker. Mr. Moore then carried out the essential spade work:

opened three bank accounts in Vienna, Austria, distinguished the casualties with the assistance of Taylor. He was presently prepared for the murder.

On a fine Saturday morning he reached the EFT department of the Primary Worldwide Bank and posing as one of the casualties he inquired the non-involved representative to exchange a strong whole to Viena. The arrange required affirmation by a moment representative. The arrange was affirmed through Taylor. The sum was exchanged from the account of the casualty to the specified outside account. The con craftsman rehashed the execution twice and within the three exchanges almost seventy millions of dollars were exchanged. It took him approximately one hour to achieve the deed. He was exceptionally upbeat at his victory.

With banks hesitating in sharing details of the person or entity who is transferring money via NEFT, it may be you next time. Although the Reserve Bank of India (RBI) has directed banks to furnish appropriate details in passbook or account statement for credits sent and received by the customer through NEFT, all the recipient gets is just a name and amount.

Social Engineering Frauds:

Social Engineering is the craftsmanship of controlling individuals to induce them to provide up private data relating to their bank accounts, computer passwords, Email-addresses, etc, in brief their ELECTRONIC Personality so that they can get to our bank accounts, computers, tablets and mobiles. Hence they are able to control and mishandle the data to require out cash and accept other noxious and destructive programs.

Data Analysis:

Based on kind of banks and category of banks, the data following is given:

Category of Bank	No of Cases	Percent
Public Sector Bank	54	91.5
Private Sector Bank	1	1.7
Cooperative Bank	3	5.1
Regional Rural Banks (RRB)	1	1.7

+ Source – Dr. Gupta & Agarwal, Cyber Laws

The above result shows that the Public Sector Banks have seriously failed in controlling or curbing the frauds in digital banking.

The crux of social engineering fraud is the environment of trust. By adopting familiar or authoritative personas, fraudsters place their victims in a comfort zone, only to breach their trust later.

An exemplary instance is the notorious ‘Jamtara scam’ from India. Here, individuals from the Jamtara district, under the guise of bank officials, would call unsuspecting victims. Using tactics of fear or enticement, they would coerce victims into revealing their banking credentials, resulting in significant financial losses for the individuals targeted.

The major and popular frauds which took place in the history of banking sector are here in below:

The PNB Fraud

The PNB fraud, which came to light in 2018, is one of the biggest managing an account embarrassments in India's history. Jewel shippers Nirav Modi and his uncle Mehul Choksi duped the bank of roughly \$2 billion through a complex web of unauthorized exchanges.

Depiction and How it Happened: The extortion was committed utilizing an instrument called a Letter of Undertaking (LoU). The pair overseen to get these LoUs from PNB without any collateral, utilizing their associations with bank authorities. They at that point utilized these LoUs to get credit from abroad branches of Indian banks. The extortion went undetected for a long time due to a need of integration between the bank's Quick framework and its center keeping money framework (CBS).

The major reason for such fraud taking place was the poor coordination between Swift and Core Banking System (CBS).

The Bank of Baroda Black Money Scam

The Black Money Scam uncovered in 2015, included the illicit exchange of over ₹6,000 crores (\$810 million) to Hong Kong beneath the pretense of purport settlements.

Portrayal and How it Happened: The trick was carried out through shell companies, which opened accounts in a Sway department in Delhi. These companies expanded the esteem of imports, permitting them to exchange expansive wholes of cash abroad without raising doubt. The bank's representatives encouraged these exchanges, bypassing the obligatory detailing necessities.

Escape clauses: The key escape clause abused in this case was the insufficient checking and detailing of suspicious exchanges. The bank representatives were able to control the framework due to frail inside controls.

ICICI Bank Loan Scam

Chanda Kochhar, the previous CEO and Overseeing Executive of ICICI Bank, was involved in a contention including a ₹3,250-crore advance (\$437 million) to the Videocon Bunch in 2012.

Depiction and How it Happened: The credit was endorsed to Videocon Gather in a quid professional quo course of action, where Kochhar's spouse, Deepak Kochhar, purportedly gotten kickbacks through a company called NuPower Renewables. The Central Bureau of Examination (CBI) affirmed that Chanda Kochhar mishandled her position to give the credit, driving to a wrongful misfortune for ICICI Bank.

Escape clauses: The case highlighted the issue of struggle of intrigued and frail corporate administration within the Indian managing an account framework, with senior bank authorities mishandling their specialist for individual pick up.

The Kingfisher Vijay Mallya Scam

The Kingfisher mogul Vijay Mallya is blamed in India of extortion and cash washing to the tune of 90 billion rupees. He fled to the UK and there are endeavors underway to urge him removed. Broadly considered to be India's reply to Richard Branson, the ostentatious Indian business person built up his acquired domain, Joined together Breweries Bunch, the prized resources of which were its refreshments division and Kingfisher Carriers, and lived a extravagant way of life, buying Equation One and cricket groups, islands and vintage cars. But the collapse of Kingfisher Carriers, which halted flying in 2012 and had amassed US\$1 billion in obligation, cleared out him in

inconvenience. State Bank of India has called for him to be imprisoned as the country's biggest loan specialist tries to recuperate cash it is owed.

The PMC Fraud

In September 2019, the Save bank of India took control of the PMC bank, and the operational administration was within the hands of the RBI for six months.

The financial specialist open begins to freeze and reach out to the closest branches. RBI at that point expanded the restrain of withdrawal to 10,000 and 25,000. Bliss Thomas, Previous overseeing chief of PMC bank, cheated the bank sheets, the evaluators, the government, and the Save Bank of India for numerous a long time by concealing the defective advance records of ₹6,500 crores. These ₹6,500 crores were taken by Lodging advancement and foundation restricted (HDIL), a genuine bequest firm.

Thomas conceded everything and attempted to clarify the circumstances beneath which he took such choices within the letter he composed to the Save bank of India. He still accepts that the Lodging improvement and foundation constrained firm will reimburse the sum, and things will get on track. He displayed the entire guide to recuperate the parts of the advance.

In his showdown, Thomas moreover said that he took this choice since HDIL and the bank have been doing trade together since 1990 and share great relations. He included that he concealed the data to protect its notoriety and the bank itself. The huge account information was not exchanged to RBI since of the chance to their name's notoriety.

In Feb 2022, the previous executive, Bal, was taken beneath guardianship.

This extortion case came to light after the Save bank of India taken note that PMC bank made invented accounts to stow away over 4,300 crore credits to the firm, which was on the skirt of liquidation at that time. Concurring to the RBI, the PMC bank secured 44 fake and risky advances, and HDIL was included in these accounts.

Legislative Framework for Digital Banking Frauds in India:

Indian Penal Code – Provisions:

Section 378, Theft

Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.

Section 409, Breach of Trust

Criminal breach of trust by public servant, or by banker, merchant or agent.—Whoever, being in any manner entrusted with property, or with any dominion over property in his capacity of a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with [imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

Section 415, Cheating

Cheating.—Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to “cheat”.

Section 416, Cheating by Personation

Cheating by personation.—A person is said to “cheat by personation” if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. Explanation.—The offence is committed whether the individual personated is a real or imaginary person.

Section 420, Cheating and dishonestly inducing delivery of property

Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall

be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 464, Making a false document.

[A person is said to make a false document or false electronic record— First —Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any [electronic signature] on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the [electronic signature],

with the intention of causing it to be believed that such document or part of document, electronic record or [electronic signature] was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or Secondly —Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with ³⁴² [electronic signature] either by himself or by any other person, whether such person be living or dead at the time of such alteration; or Thirdly —Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his [electronic signature] on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration.]

Section 468, Forgery for purpose of cheating.

Whoever commits forgery, intending that the [document or electronic record forged] shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 470 Forged [document or electronic record].

A false 1[document or electronic record] made wholly or in part by forgery is designated “a forged 1[document or electronic record]”.

Section 471, Using as genuine a forged [document or electronic record]

Whoever fraudulently or dishonestly uses as genuine any 1[document or electronic record] which he knows or has reason to believe to be a forged 1[document or electronic record], shall be punished in the same manner as if he had forged such 1[document or electronic record].

Section 472, Making or Possessing Counterfeit Seal etc.

Whoever makes or counterfeits any seal, plate or other instrument for making an impression, intending that the same shall be used for the purpose of committing any forgery which would be punishable under section 467 of this Code, or, with such intent, has in his possession any such seal, plate or other instrument, knowing the same to be counterfeit, shall be punishable with imprisonment for life, or with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Indian Contract Act, 1872:

By Section 17 of the Indian Contract Act of 1872, Fraud is defined as any of the following actions conducted by a contractual party, their connivance, or their agency to induce another party or their agency to agree. The following list of circumstances that might lead to fraud:

1. The proclamation of an untrue statement as truth by a person who does not consider that statement to be true.
2. When somebody who knows or believes something intentionally conceals it.
3. Making a promise without intending to keep it.
4. Any other behaviour intended to mislead.
5. Any deed or omissions that the law expressly declares to be dishonest.

The Negotiable Instruments Act, 1881:

Sec 45A – Holder’s right to duplicate of lost Bill

Where a bill of exchange has been lost before it is over-due, the person who was the holder of it may apply to the drawer to give him another bill of the same tenor, giving security to the drawer, if required, to indemnify him against all persons whatever in case the bill alleged to have been lost shall be found again.

Sec 58. Instrument obtained by unlawful means or for unlawful consideration.

When a negotiable instrument has been lost, or has been obtained from any maker, acceptor or holder thereof by means of offence or fraud, or for an unlawful consideration, no possessor or indorsee who claims through the person who found or so obtained the instrument is entitled to receive the amount due thereon from such maker, acceptor or holder, or from any party prior to such holder, unless such possessor or indorsee is, or some person through whom he claims was, a holder thereof in due course.

Sec 87 – Effect of Material Alteration

Any material alteration of a negotiable instrument renders the same void as against anyone who is a party thereto at the time of making such alteration and does not consent thereto, unless it was made in order to carry out the common intention of the original parties.

Punishment for Fraud:

1. Since the punishment for committing fraud consists of both a fine and an amount of time behind bars, it cannot be compounded. With the development of technology, there has been a surge in online fraud, and as a result, it is now a severe penal offence.
2. The Companies Act of 2013’s Section 447 penalises fraud. The Act has over 20 provisions that are devoted to revealing frauds perpetrated by a company’s directors, senior managerial personnel, and/or corporate officials.

3. A person who is found guilty of fraud in violation of Section 447 may receive a prison term of between six months and 10 years.

CONCLUSION:

In September 2019, the Save bank of India took control of the PMC bank, In spite of the fact that organizations can never dispose of the chance of extortion totally, it is vital to have controls that can successfully identify and anticipate extortion. Productive inner controls and information analytics can offer assistance distinguish fakes speedier and subsequently offer assistance banks constrain the misfortunes caused. The part of inner review groups is growing to incorporate extortion hazard administration. [6] An RBI circular on review and review frameworks in banks notes the disappointment of inner review groups to highlight the presence of abnormalities such as disgraceful credit examination, dispensing without watching the terms of authorize, disappointment to work out appropriate post-disbursement supervision, and concealment of data relating to unauthorized abundance withdrawals. [7] The circular has proposed an arrangement of changes to the Inside Review work to progress its adequacy beginning with growing the scope of the work itself. Inside Review groups are anticipated to particularly report on the position of abnormalities in branches, analyse and make in-depth ponders of the debasement/ extortion inclined areas,(such as examination of credit proposition, adjusting of books, compromise of connect- department accounts, settlement of clearing exchanges, tension accounts, premises and stationery accounts) amid the course of their review; in this manner clearing out no scope for any acts of neglect/ abnormalities remaining undetected. These show up to have borne a few natural product as respondents have demonstrated that they depend intensely on review/ compromise as one of their essential modes of extortion location. In spite of these changes, the characteristic nature of inside reviews tends to be restricted, depending on scrutinizing a little test measure for extortion and abnormality. [8] In such cases, extortion may proceed to be executed, in case the related exchanges drop exterior of the review test, making it troublesome to identify. In our encounter, fakes identified essentially through inner review have existed on a normal for 12-18 months, earlier to location, essentially expanding the extortion misfortune sums and making recuperation troublesome. In this setting it is curiously to note the utilize of whistleblowing

channels by banks to identify extortion. Concurring to the Association of Certified Fraud Examiner (ACFE), organizations with whistle-blower hotlines involvement fakes that are 41 percent less exorbitant, and are able to identify fakes 50 percent speedier compared to organizations that don't have such a channel⁵. In any case, in our encounter we have watched that Indian companies tend to approach whistleblowing with a 'tick within the box' mindset, regularly coming about in incapable and ineffectively overseen whistle-blower programs. The victory of a whistleblowing program lies in its appropriation by representatives and third parties such as clients and trade accomplices. For Indian banks working over distinctive geographies, it gets to be foremost to invest in a vigorous whistleblowing program that's not limited to one dialect, restricted working hours and specifically open to certain representatives (e.g. as it were mid-level workers). Assist, banks must institutionalize preparing programs to empower representatives to blow the shriek when they see or listen anything suspicious or apparently untrustworthy. [9] Another developing instrument that banks can utilize to distinguish fakes is information visualization. We are seeing worldwide selection of these advances in driving banks. Built on the introduce that human creatures acclimatize data superior in visual arrange, than numerical arrange, this apparatus gives a visual representation of information designs and exceptions to interpret multidimensional information such as recurrence, time and connections into an instinctive picture. [10] This may be valuable in distinguishing covered up and/ or circuitous connections, illustrating complex systems including numerous layers and/ or a few middle people and following the development of cash particularly in hostile to- cash washing examinations and preoccupation of reserves by borrowers. Information can too be spoken to geo-spatially, to appear intelligent between information such as budgetary exchanges, resource data, client information and contracts, references to places, names and addresses.

REFERENCES:

1. Thakur, S. (2019). Electronic Banking Fraud in India: Effects and Controls. *International Journal of Science and Research*, 8(10), 823-829.
2. Johri, N. (2021). E-Banking Frauds and Safety Solutions: Analysis. *Indian Journal of Integrated Research in Law*, 2(6), 1-12.

3. Găbudeanu, L. et al. (2021). Privacy Intrusiveness in Financial-Banking Fraud Detection. *Risks*, 9(104), 1-22.
4. Myneni S.R. “*Principles of Economics for Law Students*” Pioneer Books, Allahabad Law Agency 2nd Edition 2003. Smith Russell G., Peter Grabosky and Gergor Urbas, “*Cyber Criminals on Trail*” published by Cambridge University Press,2004.
5. Ali, M.A. et al. (2019). E-Banking Fraud Detection: A Short Review. *International Journal of Innovation, Creativity and Change*, 6(8), 67-87.
6. Kavita (2021). Analysis of Internet Banking along with Legal Aspects in India. *Kurukshetra Law Journal*, 11, 113-129.
7. Verma S.B., Gupta S.K. and Sharma M.K. “*E-Banking & Development of Banks*”, Deep & Deep Publications Pvt.Ltd. Delhi, 2007.
8. Tripathy, P., Walini “Emerging scenario of Indian Banking Industry” *Mahamaya Publishing House*, New Delhi 2005.
9. Smith Russell G., Peter Grabosky and Gergor Urbas, “*Cyber Criminals on Trail*” published by Cambridge University Press,2004.

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 hentricontane 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
