International Journal of Research in Social Sciences
Vol. 13 Issue 12, Dec 2023,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

The E-Fraud Conundrum: A Critical Examination of the Indian Landscape

Ritu Basu [*] and ***Md Ramiz Akhtar*** [†]

ABSTRACT

'Bank anytime, anywhere'- the phrase has created a radical change in the way the society has been contemplating the concept of banking through ages. With the advent of advanced technology and the considerable outreach of the internet, banking nowadays is literally 'at our fingertips'. In fact, when almost every facet of life has been pushed to the digital mode due to the world experiencing a pandemic due to COVID-19 disease, online banking has become but an inseparable part of our daily life. However, besides being fast and convenient, e-banking is cloyed with the risk of frauds being committed through the internet in a number of different forms and methods. The remarkable increase in the number of online bank fraud cases in the country has become a serious concern with banks losing huge volume of money consequent upon such offences. The legislative framework in India is not sufficiently equipped to handle such crimes specifically. The enforcement agencies and the investigating authorities are not sufficiently armed to deal with the mess that could be created by such crimes. Hence, this paper aims at highlighting the inefficiencies in the current coping mechanism and at suggesting some variations including incorporation of certain specific technological tools that can be useful in fraud detection and fraud risk management in case of an online bank fraud.

KEYWORDS: Online banking, internet, fraud detection, fraud risk management.

INTRODUCTION

A total of around 7,400 Indian bank fraud cases have been reported by the Reserve Bank of India in the financial year 2021. The total value of bank frauds amounted to 1.4 trillion Indian rupees. Although this is a slight declineas compared to the last financial year, the last decade has shown phenomenal figures both in total numbers and in value of frauds [1] (Central Board of Directors, 2021). Having been treated as a "cost of doing business" for many years, frauds in the banking sector, with its increasing frequency and complexity, have now become a serious cause of concern for regulators. In fact, "fraud" has been defined by the regulator of banks, Reserve Bank of India, as, *"A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the*

[*]Student of LL.M, The West Bengal National University of Juridical Sciences.
[†] Student of LL.M, The West Bengal National University of Juridical Sciences.

books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank" [2](Chakrabarty, 2013).

One facet of banking that has grown considerably in the past few years is the e-banking. Internet banking or e-banking has found its inception for the purpose of achieving two basicpurposes- first, increased consumer expediency and second, reduction in the operation costs for banks. A huge number of advantages have been the consequence of such a form of banking. Some of such benefits include: increase in rates of interest, looking up account details and bank statements online, bill payments in an easier way, faster transfer of money through accounts, and scheduling automatic intervallic payments. So, online banking facilitates borderless banking services anytime, anywhere and anyhow. However, frauds in the banking sector have increased immensely with the introduction of the e-banking system. In 2020, over four thousand cases of online banking frauds were reported across India[3](Number of online banking frauds reported across India in 2020, by leading state, 2021).

DIGITAL DECEPTION:UNCOVERING E-BANKING FRAUD TECHNIQUES

The fraudsters use a variety of ways to commit frauds on the banks using the internet. Unfortunately, the ones who suffer the most with respect to such frauds are the innocent customers who trust the baking system. In fact, mostly, the dormant bank accounts are the ones that are the victims of frauds. Following are a few of the significant ways in which such frauds are committed:

1. **Phishing:** Also known as brand spoofing, phishing is one of the most common forms of social engineering attacks. In this form of attack, a dummy website of any popular organization or company is created. The offender then uses emails or social media to send the fake link to targets. Now, the victim, being a legitimate user stoops into giving his / her sensitive information. The login authorizations and other personal information of users obtained by the offender are used subsequently for logging into the parent site, generally online banking sites.
2. **Spyware:**Victims, in this case, are secretly monitored through infiltration software known as spyware. This, in turn, assists a hacker to acquire personal information from the computer of the victim. Spyware functions by exploiting vulnerabilities in the application that is attached to links that are clicked by users. An example of

spywares is 'Trojan Horse'. This software unfolds when malicious software entrenches to a consumer's computer without knowledge of the consumer.

3. **Card skimming:**Card skimming involves the illegal copying and capturing of magnetic stripe and PINs on credit and debit cards. Such card skimming are common in bank ATMs or via a compromised EFTPOS machine. The details obtained are used to make fraudulent bank transactionsby encoding them onto counterfeit cards.
4. **Hacking**: Illegal access of a computer system to obtain valuable and confidential information of online banking consumers, hacking, is probably the most common method used by the offenders to commit bank frauds.
5. **ATM skimming:**ATM skimming is one of the most popular forms of attacks on online bank customers. This kind of an attack involves attaching false casings and PIN pad overlay instruments onto existing ATMs, or attaching a disguised skimming device onto a card reader entry, in conjunction with anobscured camera to capture PIN entry details.

FACTORS DRIVING ONLINE BANK FRAUDS

With the increase in technology and the dependence of almost every single person having access to internet on the digital platform for almost everything and every aspect of life, the frauds committed in the banking transactions have swiftly moved to the online segment. Now, India is one of the top countries experiencing online bank frauds. The following could be cited as some of the major reasons for the rise in cases of online bank frauds:

1. **A changing e-commerce landscape:** The world is experiencing a new trend wherein retails purchase have shifted online. A very significant development in this area is the Card Not Present (CNP) transactions, also known as remote transactions, which do not require the card to be physically present at the point of transaction. Evidently, 'cardless' transactions are an easier mode both for the user and the fraudsters. The offenders take advantage of "address verification services" in order to divert deliveries to steal information. Online skimming is a common method through which hackers gain access. Hence, when users log onto unsecured WiFi networks, thieves steal passwords and credit card information.

2. **Increasing shift to digital banking services:** Digital transformation in the banking sector is a significant modification in how banks and financial institutions gather information about, cooperate with and gratifyclients. There is an integration of digitization in every sector of banking which has changed how banks operate and how they provide service to the customers. In fact, the customers have increasingly demanded more online and mobile services from their banks. As per statistics, in financial year 2021, digital payments in India reached a total of over 53 billion Indian rupees. With regard to the cashless payment, the mobile payment app BHIM (Bharat Interface for Money) overtook debit card payments since 2018[4] (Statista Research Department, 2021). A majority of the banks and financial institutions who have moved to online transactions now have thin file credit which means they do not have much credit data. Now, essentially, less data means a greater risk of fraud.
3. **Contribution of the COVID-19 crisis:** The drastic changes in e-commerce and shifting of banking transactions to online mode due to the pandemic and the resulting lockdown has opened gateways for the offenders to commit bank frauds in a much easier way. Opportunistic hackers have taken advantage of the chaotic crisis owing to the global pandemic to commit fraudulent activity. Several fraud tactics have been used for a considerable amount of time by such fraudsters including stealing stimulus checks and unemployment benefits, collecting payments for fake COVID-19 treatments, and tricking people into donating to fraudulent charities.
4. **More refined fraud tactics:**There has been a sharp increase in the number of data breaches over recent years which have resulted in fraudsters getting easy access to personally identifiable information (PII) and using it against consumers. Fraudsters would combine real and fake data to synthesize new identities which become harder to detect. For example, for sucha purpose, a fraudster can combine address from one person and social security number of another person. With such identities, they establish open bank accounts and make use of cards, acting like legitimate customers. Once strong credit scores have been established, the fraudsters would ask for higher credit limits or larger loans and would simply stop paying. In addition, account take-overs can be affected by controlling PII. Fraudsters may obtain passwords and credentials through data breaches or social engineering

techniques and use such information to gain control over accounts and make fraudulent online purchases.

5. **Insufficiency and inefficiency of the legislation and enforcement framework:** It has often been argued that despite the presence of specific statutes addressing online bank frauds like the Information Technology Act, 2000 and certain provisions of the Indian Penal Code, 1860, such offences have increased considerably in the past few years acting as a silent killer for the society. This essentially points out that there is certain lacuna in the legislative framework of the country that fails to tackle the major crime of fraud taking place through the internet. Also, a major challenge of the country in dealing with the online bank frauds is the fact the enforcement structure and the personnel involved in the same is to a large extent untrained and inefficient.

Hence, it might be essential to look into the legislations addressing online bank frauds in India.

LEGISLATIVE FRAMEWORK: BATTLING ONLINE BANK FRAUDS IN INDIA

1. **Information Technology Act, 2000:** Various provisions of the Act deals with the management of e-banking services by the banks and measures for curbing the online bank frauds and other collateral cybercrimes. Section 3(2) provides for specific technology like "asymmetric crypto system" and "hash functions" for authenticating records, like servers and other virtual platforms by virtue of which e-banking services are provided. Further Section 72 of the Act provides for penalty in case any person discloses entrusted electronic records among other valuable documents of the bank, this causing a breach of privacy and confidentiality.

Now, internet banking does not solely involve banks and customers, rather it includes a number of third parties. Since computer networks of banks retain a lot of information about their customers and transactions including third parties, data protection provisions are very important for preventing leakage or tampering of data through sufficient legal and technical support. The Information Technology Act does include provisions about unauthorized access but it does not deal with maintenance of the

integrity of customer transactions. The legislation does not, through any provision, cast a duty upon the banks and financial institutions to protect the personal details and information of customers.

2. **Indian Penal Code, 1860:** Frauds committed in the banking sector can be prosecuted under the criminal law of the country and for such offences, adequate provisions of punishment have been prescribed under the Indian Penal Code, 1860. Some of the important provisions of the IPC in this regard are

   (i) Section 403:*"Dishonest misappropriation of property. — Whoever dishonestly misappropriates or converts to his own use any movable property, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both."*

   (ii) Section 405:*"Criminal breach of trust.—Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits criminal breach of trust."*

   (iii) Section 409: This Section of IPC prescribes punishment for criminal breach of trust by a public servant or by a banker or merchant or agent in the tune of imprisonment upto ten years.

   (iv) Section 415:*"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."*

International Journal of Research in Social Sciences
Vol. 13Issue 12,Dec 2023,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

(v) Section 463-Forgery: It is defined as- *"Whoever makes any false document or false electronic record or, part of a document, or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery".*

Evidently, no legislation in the country specifically deals with the detection, prevention, investigation and penalization of the offence 'online bank frauds'.

FRAUD RISK MANAGEMENT

The increasing number of bank frauds through the internet has called for the implementation of techniques related to fraud-risk management. CIMA (Chartered Institute of Management Accountants) official Terminology,2005 defines risk management as *"a process of understanding and managing risks that the entity is inevitably subject to in attempting to achieve its corporate objectives."* Every financial institutions including bank should form a strong fraud risk management to administer an issue of online fraud. This process includes[5](Chartered Institute of Management Accountants) many intermediary steps to achieve its goal like-

1. **Formation of a committee**- A committee of skilled persons including a chief risk officer, a non-executive director, finance director, internal auditor, heads of planning and sales, treasurer and operational staff should be formed. This committee aims to promote the procedure of understanding, detecting any preventing frauds.
2. **Identification of risky areas-** through research grey areas of transaction system as well as risky areas should be detected.
3. **Understanding and assessing the scale of risk-** On the basis of impact and occurrence of frauds, kind of fraud is detected as High(probable), Moderate(possible) and Slow(remote).
4. **Development of a risk response strategy**- The organization (the concerned banks) should make a strategy of how to accept and combat an attack in cyber system.

5. **Implementation and monitoring the suggested controls-** The committee implements some effective technologies to detect and prevent fraud.

A Chinese multinational technology company 'Alibaba' recently developed an effective fraud prevention monitoring technique as a part of their "fraud risk management system". They named this system as "Counter Terrorist Unit" or CTU which can track and scrutinize conduct of accounts or users. It can also identifyapprehensive activities and apply separate dealings based on "intelligent arbitration". It provides a digital wallet and online payment platform called 'Alipay'. The management includes five layers to prevent fraud for a transaction[6] (Jidong Chen, 2015). These are- account check, device check, activity check, risk strategy and manual review. Each of these stepsvalidates the legitimacy of every step of a transaction. A fraudster has to come through those five layers which is very tough. This could be a significant tool for prevention of bank frauds through the internet.

FRAUD DETECTION TECHNIQUE:

We have been living in the Information Age where technology advances exponentially. Around every element of the earth can be accessed through electronics media. But every access should be secured properly. Online fraud causes pecuniary as well as mental damage to victims. It should be detected prior its actual occurrence. One of the most effectivetechniques for such detection is Artificial Neural Network(ANN).

"ARTIFICIAL NEURAL NETWORK"(ANN) and "GEOGRAPHIC INFORMATION SYSTEM" (GIS):

ANN is a three-dimensional algorithm-system consisting of various interconnected artificial neural nodes, which follows the principles of human brain especially in case of pattern recognition and associative memory[7] (Masoumeh Zareapoor, 2012). Prima facie, it works as a tool of data-mining in fraud detection technique. The principle it follows is that it is trained with providing many data in its input layer which is calculated in its hidden layer using normally fuzzy algorithm and results in through its output layer.

In case of credit card fraud detection, various transactions of a particular customer are used as input data to this system which creates a specific profile of this customer. The system gets habituated to such pattern of transaction and gives expected value with least error and deviation. This is called its training mode. When a fraudster gets access to this particular

credit card, the pattern gets changed and becomes a new input to the system. Hence, the system cannot produce the expected output. Rather it fluctuates from its expected value. It produces signals and the account used is detected as a Red Flagged Account(RFA).

GIS is supplemented with artificial neural network (ANN) by providing smartforecasts of the occurrence of online fraudulent activities in the banking and financial systems[8](Dr. Eneji, Angib, Ibe, & Ekwegh, 2019, p. 709). The data of criminal activities in various hotspot areas are collected and used as input to trained ANN and it then gets processed. It results in the form of a Map indicating specific geographical coordinates where fraud-threats are predicted. The Pithburgh DMAP is such type of an artificial neural network which produces Early Warning Signal(EWS) to the administrators to analyse the crime pattern. This process is called 'gecoding'.

This is essentially similar to the system of online fraud detection that was recommended by the Reserve Bank of India through one of its circulars in the name of EWS and RFA[9] (India, 2015).However, this effective technique has not been incorporated in any functional legislation in India.

CLOSING THE GAPS: RECOMMENDATIONS FOR COMBATTING ONLINE BANK FRAUDS

Despite efforts, banking and financial institutions have not been able to succeed in identifying and convicting perpetrators of financial fraud caused online. One major cause for this is a lack of specific laws to such effect. Hence, the following recommendations are suggested for an effective handling of frauds.

1. **Formation of a specific National Policy:** The existing laws with respect to online bank frauds are evidently not sufficient enough to curb the menace of such a major offence. Hence, the authors suggest the framing of a National Policy that could address specifically the problem of bank frauds through electronic means and fill in for the gaps that exist in the current framework.The following could be cited as some of the essential features of the intended policy:

i) Incorporation of fraud detection techniques like the ANN and GIS.
ii) Creation of basic fraud management systems in the banking sectors and including prevention techniques like the CTU.

International Journal of Research in Social Sciences
Vol. 13Issue 12,Dec 2023,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

iii) Creation of an agency for coordinatingpolicies between public and private organizations for tackling fraud.

iv) Formation of a national-level unit to provide completeevaluations for the extent of losses from online fraud and calculation of risks of future threats of e-fraud.

v) Designing a "Fraud Reporting Centre" and an"Intelligence Bureau" for improved data sharing.

vi) Recognition to the duty cast upon the Banks and Non-banking Financial Companies to maintain secrecy and confidentiality for the customers' sensitive information and penalizing violation of such provision.

vii) Incorporation of an in-house Cyber Grievance Redressal Cell for the purpose of dealing with online bank frauds happening in the respective banks.

2. **Proper training to enforcement and investigation personnel:** A persistent problem with regard to the enforcement of the laws and the investigation of such a crime is the lack of training and practical knowledge of the personnel involved in such enforcement and investigation. Most officers involved have attained seniority and might not be conversant with the nuances of technology involved in the handling of online bank frauds. Hence, the authors recommend specific training programmes funded by the Government for specialized officers involved in dealing with such crimes.In fact, the Government could deliberate upon a self-governing specialized cadre of officers in accordance with All India Services, specially armed with financial and technological awareness for detecting and effectively investigating into online bank frauds.
3. **Switching to Biometric form of ATM authentication instead of PINs:** Since a lot of ATM frauds have been committed despite authentication of transactions through PINs, the authors suggest a shift to biometric form of authentication like fingerprints or retinal scan. This would reduce the risk of shoulder surfing or stealing PINs through cameras. The Biometric system offers protection against Fraudsters and also it is convenient for users to use it without having any trouble, Banks need to verify the customer's identity to provide the desirous service they want since other types of verifications like PIN and Password systems are more vulnerable towards the data breaches. Using advanced technology fraudsters got

more Tech-savvy increasing Identity theft. As per Research, in 2019 identity theft and data breaches saw a 17% of hike rate. In this scenario, the Biometric system offers end-to-end protection by which only customer can access their sensitive data.

CONCLUSION

With a lot of factors contributing to the overwhelming rise of digital frauds in the banking sector, it is significantly apparent that the odds are stacked against the victim banks and the society to avert or handle such offences. However, just as it is said, one thorn drives away another, it is in fact possible to address digital frauds with the help of new and evolving digital techniques themselves. With a fresher approach to legislation and policy issues and incorporation of necessary technological tools, the country can possibly be shielded, to some extent, if not entirely, from the ravages of huge financial scams using the internet in the banking sector. E-banking has become a part and parcel of almost every sphere of transaction especially during and post the pandemic. Banks, being one of the most essential parts of the daily life in the current times, need to absolutely safe and secure for the use of the public and the stakeholders which would otherwise lead to tremendous damage to the economic integrity of the country.

References

1.Central Board of Directors. (2021). *Reserve Bank of India Annual Report 2020-21*.

2.Chakrabarty, D. K. (Performer). (2013, july 26). *Frauds in the Banking Sector: Causes, Concerns and Cures.* New Delhi.

3.Number of online banking frauds reported across India in 2020, by leading state. (2021, october 20). Retrieved from statista:https://www.statista.com/statistics/1097957/india-number-of-online-banking-frauds-by-leading-state/.

4.Statista Research Department. (2021, July 8). *Total value of digital payments in India from financial year 2018 to 2021, by transaction type*. Retrieved from statista: https://www.statista.com/statistics/1196776/india-digital-payments-by-transaction-type/

5.Chartered Institute of Management Accountants. (n.d.). *Fraud risk management: A guide to good practice.*

6.Jidong Chen, Y. T. (2015). Big data based Fraud Risk Management at Alibaba. *The Journal of Finance and Data Science*, 1-10.

7.Masoumeh Zareapoor, S. (2012, august). Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria. *International Journal of Computer Applications, 52*, 35.

8.Dr. Eneji, S. E., Angib, M. U., Ibe, W. E., & Ekwegh, K. C. (2019, march). A Study of Electronic Banking Fraud, Fraud Detection and Control. *International Journal of Innovative Science and Research Technology, 4*(3), 709.

9.India, R. B. (2015). *Framework for dealing with loan frauds.*