

How to Cite:

Modi, S., Premani, V., & Kaur, M. (2021). A critical analysis of e-banking frauds and laws in India. *International Journal of Health Sciences*, 5(S2), 931–938.

<https://doi.org/10.53730/ijhs.v5nS2.13925>

A critical analysis of e-banking frauds and laws in India

Dr. Seema Modi

Assistant Professor, School of Law, Lovely Professional University, Punjab

Ms. Vanshika Premani

Assistant Professor, School of Law, Lovely Professional University, Punjab

Ms. Mandeep Kaur

Assistant Professor, KCL Institute of Laws, Jalandhar

Abstract---The present era is the age of science and technology. Information communication and technology has a great contribution to society. It has contributed to all spheres of society. The banking field is no exception to it. Just because of e-banking, money can be transferred at any time without waiting for the opening of banks. E-banking is therefore quite speedy and convenient. However, there is a drawback to online banking. It isn't completely safe. A significant sum of money is moved illegally through e-banking scams. A poor ordinary man makes great efforts to save money for emergency situations, but e-banking fraudsters employ every malfeasance to make money quickly and steal from the poor. There are laws in place to regulate it. True evidence of it may be found in the Information Technology Act of 2000. In addition to that, the Reserve bank also promptly releases instructions in this respect. In order to address these serious concerns, a separate complaint cell has been developed. However, it has been shown that these offences are becoming worse every day. Therefore, it is important to research it and identify a workable solution to this problem. The examination of the relevant legislation and their critical analysis has been the main subject of the researchers' work. In addition to that, the yearly reports of the relevant agencies, including the National Crime Report Bureau and the Internet Crime Complaint Centre, have also been read. The judiciary has also been paid proper attention to it. After going through all available material, the researchers have supposed to recommend some suggestions to carry on e-banking in a more effective and efficient manner.

Keywords---e-banking frauds, information technology act, financial transactions.

Introduction

Development of science and technology has transformed almost every activity into electronic mode. The early 1990s saw the introduction of banking sector reforms. Up until 1980, banks allowed consumers to conduct banking transactions through a single channel that is done in person at the bank, and as a result of the reforms, customers can now conduct financial transactions through a variety of channels, which is quicker than the manual banking process. Financial transactions are possible by just a single click.¹ The banking industry has seen a significant transformation thanks to technology. E-banking provides banking services via electronic channels. Early private sector banks were not fully computerised, whereas new private sector banks and foreign banks were from the moment of inception fully computerised.

A system where financial transactions are handled utilising information and computer technology rather than human resources is known as electronic banking, or e-banking. E-banking differs from typical banking services in that there is no direct contact between the bank and its clients. By using several platforms that may be utilised with a variety of terminal devices, such as a personal computer and a mobile phone with browser or desktop software, telephone, or digital television, banks can give information and services to their customers via e-banking.² Even if there are a tonne of benefits to e-banking, there are also a variety of challenges as a result of technical advancement in the banking industry. Operational hazards, technological problems, security problems, and legal problems are the main causes of the various difficulties encountered when using e-banking services. Unauthorized access to data, data theft by hackers, and data loss or damage by viruses are just a few of the many security challenges people encounter. In the banking industry, technological advancement coexists with difficulties. The biggest problem is one that has to do with security and law. The depository financial institution of India, serving as regulator and supervisor and taking into account the increase in e-banking fraud instances, has given instructions to the banks on how to prevent e-banking frauds from being carried out by the fraudsters. safeguard the frauds and each now so as per situational changes is making adjustments in guidelines by issuing new one. Hence To find a solution to the demographic problem that is escalating in many parts of India and across the border, an analysis of the rules and regulations relating to e-banking scams is essential. Without widespread support, laws cannot be carried out. That is supported by the failure to strictly enforce the legislation and by the observation of e-banking frauds. Fieldwork can get your hands on problem-oriented ideas that the lawmakers can embrace and fill the theoretical gaps with in order to avert future financial losses to India and potential harm to the Indian economy.

¹ Dr. C. Gupta and Abhilasha Sharma, Banking Frauds in India: Trends and Legal Challenges, International Journal of Education, Modern Management, Applied Science & Social Science (IJEMASSS), ISSN : 2581-9925, Impact Factor: 6.340, Volume 03, No. 01, January - March, 2021, pp.276-280

² Mrs. S. Kalpana and Dr. M. Mahalakshmi, Cyber Crime: A Growing Threat to Indian E-Banking Sector, Journal of Emerging Technologies and Innovative Research, (ISSN-2349-5162), December 2020, Volume 7, Issue 12

Research Objectives

- 1) To study modern ways of banking fraud in online mode.
- 2) To evaluate the international law relating to e-banking frauds.
- 3) To analyze the efficiency and weaknesses of Indian laws relating to e-banking frauds.
- 4) To study the reports of concerned international and national bodies, if they are available.
- 5) To suggest measures to curb the e-banking frauds in India.

Literature Review

Jaishree Chavan (2013) has pointed out the significance of internet banking. No doubt, internet banking has made our life convenient. It is cost-effective, time-saving, speedy and very convenient. Fund management is also very easy through it. But, along with it, it has its own challenges. The biggest challenge is towards confidentiality, integrity, and authentication. Regulation and supervision is other challenges.³

Jaspreet Singh and Neeta Brar (2012) defines internet banking as a medium through which banking services are delivered. It is a strategic tool for the growth of the business. It is widely accepted at the international level. India is gradually moving towards it. To change the perception of the customers, it is very much necessary to organize awareness programs and by making the services user-friendly, proper security, and the best responses to the services offered.⁴

Neha Dixit and Dr. Saroj K. Datta (2010) have also shown their concern about the issues relating to privacy and security. Due to lack of knowledge of information communication and technology, adult customers avoid accepting online banking services. If security and privacy are ensured, trust is created and level of awareness is increased, Indian customers will start accepting e-banking services.⁵

CA Mazrun E. Jokhi (2014) has presented the study done by Reserve Bank of India (RBI). As per the RBI, there were 1.9 crore credit card users in India till date. Approximately, Rs. 14,000 crore went through in banking transactions. The online payment market size has increased with the passage of time. Online shopping is done not only through the public bank, but via payment gateways of private banks also.⁶

³ Internet Banking-Benefits and Challenges in An Emerging Economy, International Journal of Research in Business Management (IJRBM) Vol. 1, Issue 1, June 2013, 19-26.

⁴ Internet Banking Need of Current Scenario. INTERNATIONAL JOURNAL OF MANAGEMENT & INFORMATION TECHNOLOGY, 1(2), 67-72.

⁵ Acceptance of E-banking among Adult Customers: An Empirical Investigation in India. Journal of Internet Banking and Commerce. August 2010, 15(2):1-17

⁶ Modern Form Of Older Crimes: Computer Related & E- Frauds, Volume 1, Issue 6, November 2014, International Journal of Business Quantitative Economics and Applied Management Research, Pg. No: 63 to 70

Neha Sharma and Dr. Dhiraj Sharma (2017) have properly described the issue with the use of tables and diagrams. Their study states that even the bank employees do not take the issues of fraud seriously. They neither have much awareness about it, nor pay much attention towards the guidelines issued by the RBI. One of its responsible factors is work pressure. The trained employee may tackle with the issues efficiently. There must be sufficient staff in the banks, so that the bank employees do not feel over-burdened. The communication between the staff and supervisor must be sufficient so that data relating to fraud may be effectively spread.

Upasna Ghosh (2021) has dealt with online financial frauds and cyber laws in India. She pointed out that the Information and Technology Act, 2000 contains a lot of confusion and ambiguity. The offences under cyber laws are bailable in nature. They become non-bailable only when they are combined with the non-bailable offences mentioned under the Indian Penal Code. Today, spam has become a very big issue, regarding which India is not having any law.

Research Methodology

For doing the study, the researchers will follow the descriptive method to discuss the existing legal system. It will be followed by the exploratory method to explore new mechanisms and systems. Then, the cause-effect relationship will be found out to suggest the solution to the problem. The doctrinal method will be adopted to do this study. The data will be collected through secondary sources. For the collection of data, the researchers suppose to go through the related statutes, judicial decisions, reports of the committees and guidelines issued by the Reserve Bank of India. If the need is felt, any other source may also be gone through, like official websites etc.

Indian laws relating to E-banking Frauds

The country's financial needs are believed to be supported by the banking industry. It makes a significant contribution to the expansion and growth of a country's economy. This industry has aided in the floatation of currency by encouraging the general public's savings and investing habits. Banks are the primary foundation of financial stability, one can readily claim nowadays. It would be fair to argue, however, that more frauds have been recorded as a result of the expansion of banking operations and people's reliance on banks to meet their financial demands. Both traditional and internet scams are among the crimes.

With the advent of technology and digitalization in every sector, life has become easy. Banking sector just like any other sector has provided a number of technological options and facilities to its customers. Today much of the work undertaken by banks has been digitalised. Nonetheless, with the many advantages technology has brought at the disposal of the banking sector, India has witnessed a drastic rise of frauds in e-banking transactions. Some most probable reasons for the rise in e-banking frauds are:

- Rise in online transactions since the last decade.
- Lack of awareness amongst the customers
- Lack of security features
- Illegal Hacking

- Lack of stringent data protection systems installed
- Lack of data protection laws

The relevant laws that provide for the legal framework for banking in India are: the Banking Regulations Act, 1949, the Reserve Bank of India Act, 1934, and the Foreign Exchange Management Act, 1999. The Reserve Bank of India is the central regulatory body which issues license to all the banks. In other words, no banking institution can function as a bank in India without obtaining a license from Reserve Bank of India (“RBI”). The power to grant license has been conferred upon RBI under Banking Regulations Act, 1949. Various types of activities which a bank may undertake and other prudential requirements are provided under this Act. Accepting of deposit from public by a non-bank attracts regulatory provisions under Reserve Bank of India Act 1934. Under the Foreign Exchange Management Act 1999, no Indian resident can lend, open a foreign currency account or borrow from a non-resident, including non-resident banks, except under certain circumstances provided in law. Besides these, banking activity is also influenced by various enactments governing trade and commerce, such as, Indian Contract Act, 1872, the Negotiable Instruments Act, 1881, Indian Evidence Act, 1872, etc.⁷

As per RBI report on Internet Banking, 2001:

“Internet banking is an extension of the traditional banking, which uses Internet both as a medium for receiving instructions from the customers and also delivering banking services. Hence, conceptually, various provisions of law, which are applicable to traditional banking activities, are also applicable to Internet banking.”

However, there has been a lot of questions put to the legality of internet transactions in particular and use of electronic medium in general. The validity of an electronic message / document, authentication, validity of contract entered into electronically, non-repudiation etc. are important legal questions having a bearing on electronic commerce and Internet banking. The report had also doubted the efficiency and ability of banks in complying with legal requirements concerning secrecy of customers account, privacy, consumer protection etc. given the vulnerability of data / information passing through Internet. There is also inadequacy of law to deal with situations which are technology driven like denial of service / data corruption because of technological failure, infrastructure failure, hacking, etc. There are various jurisdictional issues and conflict of laws of different nations that arise in cross-border transactions done through Internet.

Amendment to the Indian Penal Code, 1860⁸

“After Chapter XXII, the following shall be inserted:

Chapter XXIV

512 - Financial Fraud – Financial fraud means and includes any of the following acts committed by a person or with his connivance, or by his agent, in his dealings with any bank or financial institution or any other entity holding public funds;

⁷ <https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=243#ch7> (as visited on Jan. 10, 2021)

⁸ <https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=248> (as visited on Feb. 25, 2021)

- a) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
- b) the active concealment of a fact by one having knowledge or belief of the fact;
- c) a promise made without any intention of performing it;
- d) any other act fitted to deceive;
- e) any such act or omission as the law specially declares to be fraudulent.

Provided that whoever acquires, possesses or transfers any proceeds of financial fraud or enters into any transaction which is related to proceeds of fraud either directly or indirectly or conceals or aids in the concealment of the proceeds of financial fraud, commits financial fraud.

(f) 'A', a computer engineer is engaged by a bank to repair the computers. 'A' transfers funds from the accounts of the customers of the bank by means of electronically operated system and without any authority from the bank. 'A' is guilty of financial fraud.

Amendment

513(a) - Punishment for Financial Fraud

Whoever commits financial fraud shall be:

- a) punished with rigorous imprisonment for a term, which may extend to seven years and shall also be liable to fine.
- b) (b)Whoever commits serious financial fraud shall be punished with rigorous imprisonment for a term which may extend to ten years but shall not be less than five years and shall also be liable for fine up to double the amount involved in such fraud.

Provided that in both (a) and (b) all funds, bank accounts and properties acquired using such funds subjected to the financial fraud as may reasonably be attributed by the investigating agency shall be recovered and restored to the rightful owner according to the procedure established by law.

Explanation : (1) Public fund means funds collected from public either by deposit or by issue of equity or loan instruments or through public investment in any scheme or the Government fund or any amount collected from public otherwise.

Explanation : (2) For the purpose of this section, serious financial fraud means if and only if, the case (i) involves a sum exceeding Rs.ten crore; or (ii) is likely to give rise to widespread public concern; or (iii) its investigation and prosecution are likely to require high specialized knowledge of financial market or of the behavior of banks or other financial institutions; or (iv) involves significant international dimensions; or (v) in the investigation of which there is requirement of legal, financial, investment and investigative skills to be brought together; or (vi) which appear to be complex to the regulators, banks, Union Government or any financial institution.”

Suggestions

There is no use to explore the issue, if some solutions are not supposed. The Reserve Bank of India also makes the study time-to-time and makes recommendations.

Those studies have been thoroughly gone through before giving the following suggestions:

- 1) Everyone must make sure that all devices and accounts must be password secured. The password must not be disclosed to anyone in any situation.
- 2) The most recent versions of an antivirus program and a firewall should be installed on all computers and laptops.
- 3) On insertion of ATM card into machine, card skimmers steal the data of the card. This stolen data is then utilised to make a cloned card. Your account can be accessed with that copied card. These Skimmers are challenging to find. Therefore, before inserting your card, you must thoroughly and actively inspect the device for card skimmers.
- 4) Before putting a security policy into effect, banks must have a security policy that has been authorised by the board of directors. The knowledge system through which e-banking transactions are carried out must be protected by a separate department, and the data recorded in the system must have high security.
- 5) According to RBI guidelines, every Indian bank and foreign bank with a branch in India must have a separate department that is solely responsible for managing banking frauds. These departments must also either resolve any cases that come to the bank's attention or provide guidance to customers on how their cases can be resolved, the fraudster can be apprehended, and the money can be recovered.
- 6) Each bank, financial institution, and intermediary is required to create a Best Practice Code (BPC) within the time range specified by the regulator for its officers and personnel in order to offer a detailed rule-based procedural framework in customer-related situations and the application of judging power. There must be internal training in this regard. Alongwith it, the regular inspection must be there to ensure the proper compliance.
- 7) Banks must inform their clients of the risks associated with utilising online banking services and the precautions that need be taken to avoid them. The RBI states that it is the responsibility of the bank to inform its customers about the precautions that should be taken when utilising internet banking services. Such information must be available on the bank's online portal. Additionally, the bank must post such information in a location that is easily accessible to customers. By sending texts to the mobile number of a customer registered with the bank, a bank can frequently and promptly alert its customers about preventive actions.
- 8) Banks must warn customers about the precautions they should take while utilising e-banking services. The bank should display this information in a suitable location where the customer may easily access it.
- 9) The incentive and promotion policies for the bank offices may be correlated in some way with the compliance of all rules and regulations made to deal with e-banking frauds.
- 10) The CBI and the Police, the investigating authorities, spend an excessive amount of time to finish an investigation and close a case. Given this, if the RBI followed up on every single fraud case to its logical conclusion, it would be dispersing its supervisory resources too thinly. The fraud reporting system needs to be streamlined in order to avoid duplication of effort and to

ensure that only the information required for the Reserve Bank of India to carry out its regulatory and supervisory duties is reported.

- 11) A separate statute may be made to criminalise financial frauds, including e-banking frauds. In the statute, the special procedure may be prescribed to deal with the cases. It will help in the speedy disposal of cases in more effective manner.

Conclusion

Online transactions are simple, convenient, and money-saving. These features make it more popular for individuals to engage in digital fraud. It may be deduced by interrogating persons of all ages that con artists are constantly looking for ways to take people's money. Netizens need to handle their personal data with care and be extra vigilant about their technological rights. Though there are some laws to deal with e-banking frauds, those laws are not so effective. There is need for a strong and specific legislation which may particularly deal with e-banking frauds. Information Technology Act, 2000 may be applied only with the Indian Penal Code, to carry on the proceeding in case of e-banking frauds. Indian Penal Code does not define the word 'fraud', nor it deals with digital financial frauds. So, making of specific and independent legislation is direly needed to deal with the problem effectively. The Reserve Bank of India also makes the study time-to-time and makes recommendations. In 2001, The Report of its Expert Committee on Legal Aspects of Bank Frauds was issued, the Chairman of this committee was Dr. N.L. Mitra. He has also recommended the same. To stop the occurrence of scams, it is also necessary to raise global awareness, educate people, and promote users' rights.