AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

A STUDY ON THE LEGAL ACTION TAKEN FOR E-BANKING FRAUDS BY GOVERNMENT OF INDIA

Mr. AJAY D. PATEL,
Research Scholar
Adhyapak Sahayak from V.T.Choksi Sarvajanik Law College Surat
Dr. Vikaram Desai
Guide
Veer Narmad South Gujarat University, Surat, Gujarat.
Email – ajay.patel873@gmail.com

Abstract

Online banking not only provides users with greater convenience, but also gives financial institutions a leg up on the competition. However, the fraudulent actions of fraudsters have brought focus to the security of e-banking; the lack of proper e-banking security has prevented many individuals from using the service to this day. The presentation presents a summary of the difficulties in ensuring safe online banking. The difficulties and traits of online banking deception have also been duplicated. In addition, this report surveyed several methods now in use for the prevention and detection of extortion and attacks on e-banking services. E-banking, or electronic banking, in India has seen a variety of shifts as a result of technological advancements. Different innovations have happened in the banking sector, such as the introduction of cards, the introduction of the Electronic Clearing Service, the introduction of the Electronic Assets Transfer, and the notion of online banking and mobile banking. Electronic banking, or "E-Banking," is a catch-all phrase for various types of banking conducted via electronic means, such as the internet, telephone, mobile phone, etc. The bank, via E-Banking, must present the fundamental idea of IT-based Enabled Services to its customers. Additionally, it was a huge shock to the standard banking

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

system. Debit and credit cards make financial transactions easier for consumers. E-banking is growing rapidly in India because more and more people have access to the internet. Most people today would rather utilise an electronic medium to conduct their banking because of the many benefits it offers. While this has its benefits, it has also given rise to new problems in the realm of cybercrime, such as identity theft, phishing, credit card fraud, and so on.

Keywords: *E-Banking, Cyber Crime, Legal Action , IT*

1. Introduction

The rapid growth of computer and data technology (telecommunications systems and the Internet) during the past few decades has facilitated the expansion of electronic commerce on a global scale. These innovations have made it easier for businesspeople to communicate with their clients and collaborate with other companies, both inside and outside their respective fields. To facilitate a smooth flow of information between companies, to meet the demands of customers, and to gain a competitive edge, businesses rely on the infrastructure provided by electronic commerce, which incorporates information management, correspondence, and security services. Similar to many other industries, the banking industry makes use of ICT to offer its consumers more convenient and secure services. Their online banking platform guarantees efficient communication with their clients, which in turn makes it easier to set up a wide range of services for those clients. With so many names for it in the literature, it's no surprise that e-banking (also known as electronic banking, online banking, or virtual banking) refers to financial dealings conducted using information and communication technologies. When we talk about "e-banking," we're referring to the process of coordinating financial services from a location other than a physical bank.

However, as expected, e-banking presents a number of difficulties for bank management and, more broadly, for public and international supervisory and regulatory bodies. Increased reliance on ICT and transnational transactions are two major causes of e-notoriety banking's as a source of tension. Other difficulties stem from concerns over conformity, lawfulness, operations, reputation, discomfort, and safety. To ensure the safety of their customers' online banking activities, financial

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

institutions are struggling with how to create a secure information and communication technology (ICT) environment. With more and more people transacting their money online on a regular basis, there has been an uptick in bank fraud and cybercrime as a result of the prevalence of sophisticated hackers who have gained access to banking information systems and are using them to break into personal and business accounts. Online banking is vulnerable to attacks from both inside and outside the system, therefore regulators must take precautions to protect clients' privacy and keep transactions safe.

A change in perspective in the banking sector's operation has been brought about by the shift towards digitization, supported by technical developments and astute system revolutions. Banks that have historically relied on human labour are increasingly adopting automated systems; in other words, traditional banking is giving way to E-banking. Continuously, the convenience of banking is a boon to the customer base. Since the introduction of Internet banking, the fundamentals of banking have undergone profound transformations. It has allowed for banking to spread to hitherto inaccessible areas of the country. Geographically restricted banks have become available 24/7/365. Constantly, advancements in technology have made banking more convenient. Banking transactions, which were formerly limited to bank branches, can now be completed at any time, in any location, and via any device, be it an ATM, a personal digital assistant, or a computer.

E-banking fraudsters are on the rise, though, creating chaos for customers. They're getting louder and more impressive as they unveil new forms. The problem of e-banking fraud is serious and has to be addressed as soon as possible. This is a job for the government and the RBI on the macro level, and for individual banks on the micro level.

2. Review of Literature

In Brar & Singh (2012) When asked why they don't utilise internet banking, 70% of respondents said it was because they feared becoming victims of e-banking scams. This demonstrates a serious security threat as well as potential legal complications. A lack of trust in online banking services has discouraged customers from making use of them. According to the results of the study,

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

customers are not required to utilise e-banking services and, if the deception is done, they stand to lose money. Customers report that if they start using, or are already using, their banks' e-banking services, they have a high risk of encountering the challenges and issues associated with e-banking fraud.

According to Chavda's (2014) research, an increase in e-banking cheats can be attributed, in part, to the fact that many Indians lack the computer literacy necessary to make effective use of e-banking services; if they do want to use these services, however, they will need the assistance of an outsider, which can result in the customer's revealing his confidential information to fraudsters. In order to reduce the risk of falling victim to e-banking scams, computer literacy is a prerequisite for using these services.

According to an article published in 2014 by Doiphode, the bank staff responsible for maintaining and regulating the e-banking system should be appropriately taught and recruited. Therefore, it is generally recommended that the positions in the e-banking system's operation, control, and caretaking be filled by people who are honest and committed to their profession. Most often, the fraudster is able to perpetrate the misrepresentation with little difficulty since the staff caring for the e-banking system is either unqualified or has the experience to handle the upkeep of the system. If the person nominated to this position does not handle his or her transactions with the electronic banking system with the utmost care, the individual's money is at risk.

The number of recorded cases of phishing in 2011 was around 26,402, according to an article by Hussain and Srivastava in 2014. Customers fall victim to fraudsters' deceptive phishing, malware-based phishing, session capture, information theft, and Space Name System-based phishing, etc., because of a lack of education and understanding on the part of customers and technology concerns. Customer education via awareness campaigns and advertisements that warn recipients to avoid clicking on links in unsolicited emails is one solution. This is the most common and straightforward form of extortion, as victims fall for emails promising them prizes or rewards, only to be duped into providing their financial information.

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

Despite the convenience of online banking, low security levels, the possibility of extortion, and a lack of guidance for operation are keeping 38 percent of clients away (Jagtap, 2014). It's found that customers' fears about the security of online banking prevent them from using the service even when they have adequate knowledge to do so. The rise in e-banking misrepresentation incidents can be directly attributed to the inadequate education, training, and direction given to banking staff. The widespread prevalence of e-banking fraud is at least partly attributable to the fact that the underlying technology hasn't been kept up to date and security standards haven't been maintained.

According to the report from 2009, the Reserve Bank of India has organised a working group led by Jamwal and Padha to find out the difficulties associated with online banking. The group agreed that the most pressing problems are those of technology and security, law, and oversight and regulation. The various rules that banks in India are expected to follow were formulated by the Reserve Bank of India (RBI) based on a report written and submitted by a working meeting. Although banks have pledged to follow the RBI's standards, so far their efforts to manage and prevent e-banking fraud have fallen short. This may be in part due to customers' lack of compliance. Thus, incidences of e-banking cheaters are on the rise every year, despite advice offered to adopt safety and security precautions and banks doing the same. The article explains the various measures the government has taken to curb e-banking fraud.

3. Methodology of the Study

In order to write the review, we relied on data collected from secondary sources. Books, diaries, newspapers, and official government websites are examples of this. The purpose of this review is to examine the idea of electronic banking, the services it provides, the laws and rules governing electronic banking in India, and the recommendations made by the Reserve Bank of India (RBI) for combating fraud in this area. Following the foregoing explanation, we feel compelled to offer certain precautionary precautions.

3.1. E-Banking

Some key terms related to online banking are defined below:

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

S. Singh, 1996, "In this context, "electronic banking" refers to the use of technology that enables clients to access banking services electronically, such as paying bills, transferring funds, viewing accounts, and obtaining data and advice. In this context, "electronic services" means any and all services accessible to users via electronic devices such as phones, computers, televisions, and the internet."

According to Rao (1997), "Electronic Banking Consists of a Wide Range of Bank Services that Rely on Information Technology."

Electronic banking, as defined by the Bank for International Settlement (1999), is the delivery of retail and low-value banking products and services via electronic channels.

Yogendres "Y. (2000), When a customer receives banking services via electronic means at his place of business or residence, the practise is known as "Electronic Banking."

3.2. Products and Services Provided by E-banking in India

The following e-banking products and services are provided by Indian banks to their customers:

- Automated Teller Machines (ATMs)
- Internet Banking

3.3. E-Banking Frauds and RBI Guidelines

- Mobile Banking
- Phone Banking
- Telebanking
- Electronic Clearing Services
- Electronic Clearing Cards
- Smart Cards
- Door Step Banking

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

- Electronic Fund Transfer

3.4. The Facilities that E-banking Offers are:

- **Convenience:** Banking has become easy with e-banking. It offers customized services anywhere anytime simply a tick of a button. With Complete you're banking at your convenience in the solace of your home.
- **No more Qs:** The need for customers to wait in long lines at financial institutions has been eliminated. Electronic banking allows for the swift completion of financial transactions.
- **24x7 Service:** e-banking provides service around the clock I,e,.,24 hours aday, 7 days a week and 52 weeks a year.

3.5.In an e-Banking environment, security threats largely fall into the following categories

- **Login Detail Disclosure:** The most commonly used by the criminals through whom they acquire login details like number, PIN which is enough to access anyone's account and steal money.
- **Computer Spy Viruses:**Viruses are malicious computer programmes that spread rapidly via electronic communication. When a customer clicks on a malicious link in an email, a malicious application is automatically downloaded and installed on their machine. To facilitate crimes like credit card cloning and fraudulent asset transfers, these initiatives collect login ids and other financial data.
- **Dummy Sites:**Criminals may trick customers into entering their credentials by creating a website that appears suspiciously like a legitimate bank's website.
- **Loss of Personal Relationship:**Since e-banking transactions don't occur in person, customers often feel uneasy about the reliability of the process and the outcomes they expect. To make up for this, e-banks must provide high-value products and services while cutting operational costs to stay competitive, which may further diminish opportunities for developing meaningful connections with consumers.
- **Organizational Structures and Resistance:**For e-banking to be successful, there must be extensive top-level organisational and management shifts. Since change is rarely embraced

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

within organisations, this could affect morale. There is a decline in project success when a change management approach is in place.

- **Trust Issues:**A lack of customer trust is another major barrier to the expansion of electronic banking. Because of safety concerns, they are hesitant to disclose private information. Customers have good reason to be wary of banks because, in certain situations, bank employees won't even aid if there's been a theft. Consequently, fewer people are making use of online banking services.
- **Change Management Issues:** Adaptation to e-banking requires major changes in the organizational structure. The reasons being technical drawbacks, high start-up cost and strategically issues.
- **Ethical Issues:**Human data privacy and security, data accuracy, data ownership and intellectual property, data accessibility, and ethical considerations around data use may be the most important issues here. Related topics include autonomy, openness, and not aiding others' deception (in unethical or unlawful ways).

4. Experimental Result

Table: 1. Digital Payments - Progress Report May 2018

	2015-16 April- March	**2016-17 April-March**	**2017-18 April- March**	**Growth Rate**
Volume (Million)	6035.7	20817.5	2.745.54	20.54
Value (Billion)	2632314	265.002.42	100.142.23	24.87

Table: 2. E-banking Fraud Cases Registered and the Amount Involved Report as per RB

	2016-17	2017-18
Number of fraud cases	6.202	14.700
Amount involved (related to credit/debit cards and e-banking)	Rs.54.40 crores	Rs. 258 crores

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

From 2016–17 to 2017–18, as shown in the above table, there was a significant increase in the number of misrepresentation cases registered under e-banking, with the amount involved likewise very huge, increasing from Rs.45.50 crores in 2016–17 to Rs.179 crores in 2017–18, or nearly three times the amount involved in 2016–17. This is a serious issue that needs to be answered as soon as possible.

Table: 3. State wise E- banking Fraud Cases Registered and Amount Involved

States	Cases Registered	Amount Involved (Rs. In Crores)
Maharastra	270	23.20
Haryana	327	8.25
Karnataka	332	7.16
Tamil Nadu	307	3.27
Delhi	265	2.34

E-Banking Frauds and RBI Guidelines

4.1. Legal Provisions on E-Banking in India

The financial industry has been significantly altered as a result of liberalisation, privatisation, and globalisation. The shift from physical to digital banking has created space for new entrants. Threats to conventional banking are growing as a result of a confluence of factors, including increased competition and technology innovation, and the emergence of a technologically sophisticated and disruptive revolutionary system. Robust banking sector legislation is required. This does not solve the issues, so more laws and regulations must be presented to address the challenges of electronic banking.

4.2. The Legal Framework for Banking in India is provided by a set of Enactments, viz

The Banking Regulation Act, 1949

The Reserve Bank of India Act, 1934 and

Foreign Exchange Management Act, 1999

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

Indian Contract Act, 1872,

The Negotiable Instruments Act, 1881,

Indian Evidence Act, 1872, etc.

4.3. The following are the obligation of the banks based on the provisions of the above acts:

- If you want to open a bank in India, you need to comply with the Banking Regulations Act, 1949, which mandates that you obtain a licence from the Reserve Bank of India.
- This Demonstration lays out the various prudential standards that banks must meet, as well as the various activities that banks may engage in.
- Non-banks in India are required to follow rules set by the Reserve Bank of India if they want to take deposits. Except in certain circumstances specified by the Act, non-resident Indians are permitted to borrow from, open an account with, and receive funds from any Indian bank, including a non-resident Indian bank.

4.4. Guidelines by RBI to Control Risk Due to E-Banking

- **Benami Accounts**

Bankers are under legal obligations to not to keep any anonymous account or accounts in fictitious name or in the name of persons whose identity is not disclosed

- **Threshold limit**

Banks need to pay extra attention to transactions involving unusually large quantities or other forms of unexpected activity. The banks need to determine the key indicators for such records depending on the specifics of their clients' profiles, organisational structures, asset pools, etc. Bullion and jewellery stores should have their records reviewed often. Periodically, suspicious activity reports (Str) must be reported to the India Financial Intelligence Unit (Balance IND). Once again, it is necessary to reevaluate the classification of risks on a regular basis.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

- **Monitoring**

Companies engaging in Staggered Marketing must have their records scrutinised on a regular basis since they invest public funds with the expectation of increased earnings. Financial institutions have a duty to notify the Reserve Bank of India and Blade - IND if they become aware of any suspicious activity, such as a large number of checks with identical dates and dollar amounts.

- **Risk Perception Parameters**

Customers should be categorized as low, medium and high risk based on the nature of business activity, location of customer and his clients, payment mode, status in the society

- **KYC Adherence**

The internal Audit ought to be well versed with KYC policies and procedures. They ought to check KYC procedures followed in the branches and comment on the weaknesses if any. Further, this must be noticed to the Audit committee of the Board on quarterly premise.

5. Conclusion

The banking industry's perspective has shifted due to the advent of online banking. Through online banking, customers get round-the-clock access to their account information. Facilitating instantaneous asset transfer to any location in the world promotes the expansion and growth of international trade and business. It has given the company a whole new perspective. Due to the advancements in Data Technology and e-banking, the banking industry in India has undergone considerable changes in recent years. Many researchers have proposed many strategies for detecting and preventing misrepresentation; some of these strategies are useful for improving the accuracy of extortion detection and prevention, while others are not. However, as of right now, there is no one approach that will reliably detect and prevent a vast array of attacks on e-banking platforms.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

References

1. *A R Raghavan & Latha Parthiban, Effect of Cyber Crime on Bank's Finances, Vol. 2(2) Feb 2014 p 173-178 < http://ijcrar.com/archive-6.php > accessed on 14th may, 2018.*
2. *Abu-Shanab, E. & Matalqa, S. (2015). Security and fraud issues of e-banking. International Journal of Computer Networks and Applications, 2(4): 179-188.*
3. *Alaba, F. A., Hakak, S., Khan, F. A., Adewale, S. H., Rahmawati, S., Patma, T. S. & Herawan, T. (2018). Model-based testing for network security protocol for e-banking application. In Information Systems Design and Intelligent Applications (pp. 740-751). Springer, Singapore.*
4. *Brar, T. P. S., Sharma, D. & Khurmi, S. S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research, 6: 127-132.*
5. *Camilleri, Silvio J. & Others. (2014). Service quality and e- banking serviceperception of maltese retail bank customers.*
6. *Davis, B. E. (2017). U.S. Patent No. 9,800,550. Washington, DC: U.S. Patent and Trademark Office.*
7. *Dr. amith varma, cyber crimes in india,central law publications, 1st ed, 2012.*
8. *Dr. lakshmi bhai, 'e banking in india- problems and prospects' ISBN- 2394, volume 5, 2018*
9. *Karimzadeh, 'electronic banking challenges in india' published in interdisciplinary journal of contemporary research in business' volume 4,2012, p.p-31-45*
10. *Mallory malesky,'traditional banking vs electronic banking systems' available at/https://accountlearning.com accessed at 18/05/2018*
11. *Ostern Pvt.Ltd. & Anr vs State Of West Bengal & Ors, AIR 2014*
12. *RBI new guidelines to customers against online fraud written by deepika uploaded on 2017 available at https://www.oneindia.com accessed at 22/05/2018*
13. *Role of RBI in indian banking system, available at https;//www.quora.com accessed at 20/05/2018*

ISSN:2320-3714
Volume1 Issue 1
Janauary 2023
Impact Factor:11.7
Subject: Commerce

14. *Vikas chauhan,' internet banking challenges and opportunities in indian context' published on journal of management science and technology, 2015, ISSN 2347*

15. *Virgillito, D., Understanding Online Banking Cyber Crime | Massive Alliance. Available at: https://www.massivealliance.com/2013/.../understanding-onlinebanking-cyber-crime/ [Accessed June 13, 2018].*

******