
E-BANKING FRAUDS AND FRAUD RISK MANAGEMENT UNDER THE LIGHT OF RBI GUIDELINES

Rachna, Research Scholar, Law Faculty, S.S.J. Campus, Almora Kumaon University, Nainital,
Uttarakhand

ABSTRACT

Indian banking system can go cashless with the aid of internet banking. Internet banking is also known as e-banking or online banking or virtual banking. It is an electronic payment system that enables customers of a bank or other financial institutions to contact a range of financial transactions through the financial institution websites. Through Internet banking we can check our transactions at any time of the day as many times as want to. The online banking frauds in India have increased tremendously. Internet banking frauds is a fraud or theft committed online technology to illegally remove money from a bank account and or transfer money to an account in a different bank. Internet banking Fraud is a form of identity theft and is usually made possible through techniques such as phishing, lottery fraud scam etc. In India there are no sufficient Internet banking laws but the reserve bank of India has issued some guidelines at the latest in this regard though it is not sufficient to make the banks follow robust and required cyber security procedure. The paper is focused to study and highlights the types and many ways of Internet banking frauds that take place in our banking systems nowadays, and also to understand and study the ways of fraud risk management on the part of every individual bank and RBI guidelines with special reference to legal framework that is prevalent in India the customer against the menace of it.

Keywords: Internet Banking, Core banking, E-banking fraud, fraud risk management, legal issues

INTRODUCTION

“India has seen a dream of digital India. From latest science to latest technology, everything should be available at tip of one’s finger”

- Narendra Modi

There is a saying that Rome was not build in a day, so is banking system of the world. Monetary policy of any country is directly related to economic development of the country where banks play major role. It is vital for any nation as it provides for the needs of credit for all the sections of the society. Banking has become more complex with the introduction of electronic banking.

E-banking is product of the last century due to research conducted in the field of banking and financial services. The concept of e-banking has been simultaneously evolving with the development of the World Wide Web programmers working databases came up with the idea of online banking transactions sometimes during the 1980s in Europe. They called this home banking. In 1983, the Nottingham building society commonly abbreviated and referred to as the Non banking service launched the first internet banking service in United Kingdom. The first online banking service in United States was introduced in 1994. In India internet banking arrived in the late 1990s. ICICI was the first bank to champion its usage and introduced internet banking to its customers in 1996. With lower costs and increase awareness about electronic media, online banking established itself only in 1999.

Nowadays Information technology has a necessary tool in banking or financial organizations. Indian banking industry has witnessed a tremendous development due to sweeping changes that are taking place in the information technology. E-banking has numerous advantage attached to its usage. It provides a platform for anytime, anywhere banking. Where there is no need for the customer to visit banks personally.

AIM OF THE STUDY

1. To understand the various E-Banking services products adopted by India.
2. To highlight the various ways of E-Banking frauds done by fraudsters.

3. To understand and study the ways of E-Banking frauds Risk Management.
4. To analyze the role of RBI's guidelines to safe banking practices.

RESEARCH QUESTION

Whether E-Banking laws in India like IT Act, 2000 and RBI Act, 1934 or guidelines given by RBI to safe banking practice, fraud Risk management are effectively address all the legal and security concerns in banking sector?

RESEARCH METHODOLOGY

The research is primarily doctrinal research. Here the data collection is necessarily secondary data which collected from books, journals, articles, law reports, newspapers, e-sources for the purpose of this study.

CHAPTERIZATION

CHAPTER ONE – E-Banking – A general overview

CHAPTER TWO – Cyber crime (fraud) and its impact on E-Banking sector.

CHAPTER THREE – E- Banking Laws in India and Fraud Risk Management

CHAPTER FOUR – RBI role in the legal and security concerns in banking sector

CHAPTER I

E-Banking – A General Overview

In e- banking, ‘e’ stands for electronic and the banking has been defined as ‘an acceptance of money from the public, for purpose of lending or investment of money, which is withdrawable by cheque, draft or otherwise’¹ and banking by using electronic devices is e-banking.

E- Banking has been defined in law lexicon as banking activities accessed by using a computer, employing and telephone.²

Electronic banking has many names like e banking, virtual banking, online banking, or internet banking. It is simply the use of electronic and telecommunications network for delivering various banking products and services. Through e-banking, a customer can access his account and conduct many transactions using his computer or mobile phone. In this chapter, we will look at the importance, features, benefits, challenges and types of e-banking services.

E-banking in India

The credit of launching internet banking in India goes to ICICI bank, since 1997. The ICICI Bank first offered internet banking services, and Citibank and HDFC bank followed with internet banking services in 1999. Today, most new-generation banks offer the same to their customers. In fact, all major banks provide e-banking services to their customers. The Government of India enacted the IT Act, 2000, which provided legal recognition to electronic transactions and other means of electronic commerce. The Reserve Bank of India is monitoring and reviewing the legal and other requirements of e-banking on a continuous basis of ensure that e-banking would develop on sound lines and e-banking related challenges would not pose a threat to financial stability.³

Internet banking has become very important nowadays you can guess it according to its number

¹ Section 6 of banking Regulation Act, 1949

² P. Aiyar Ramnath, Advanced Law Lexicon,(4th Ed.) (Nagpur; wadhwa and co;2013), p.1561

³ Jaro Jasmine and Aswathy Ranjan, A critical study on concept of E-Banking and various challenges of IT in India with special reference to RBI;s role in safe banking practice,issn:1314-3395

of users. The online banking users in India to reach 150 million by 2020 according to a study.⁴

Popular services under e-banking in India

- ATMs (*Automated Teller Machines*)
- Telephone Banking
- Electronic Clearing Cards
- Smart Cards
- EFT (*Electronic Funds Transfer*) System
- ECS (*Electronic Clearing Services*)
- Mobile Banking
- Internet Banking
- Door-step Banking

Further, under Internet banking, the following services are available in India:

1. **Bill payment** – Every bank has a tie-up with different utility companies, service providers, insurance companies, etc. across the country. The banks use these tie-ups to offer online payment of bills (electricity, telephone, mobile phone, etc.). Also, most banks charge a nominal one-time registration fee for this service. Further, the customer can create a standing instruction to pay recurring bills automatically every month.
2. **Funds transfer** – A customer can transfer funds from his account to another with the same bank or even a different bank, anywhere in India. He needs to log in to his account, specify the payee's name, account number, his bank, and branch along with the transfer

⁴ www.financialexpress.com

amount. The transfer is affected within a day or so.

3. **Investing** – Through electronic banking, a customer can open a fixed deposit with the bank online through funds transfer. Further, if a customer has a demat account and a linked bank account and trading account, he can buy or sell shares online too. Additionally, some banks allow customers to purchase and redeem mutual fund units from their online platforms as well.
4. **Shopping** – With an e-banking service, a customer can purchase goods or services online and also pay for them using his account. Shopping at his fingertips.

CHAPTER II

Cyber Crime (fraud) and its impact on E- Banking sector

The uses of internet services in India is growing rapidly. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Criminal activities in the cyberspace are on the rise. Computer crime are criminal activities, which involve the use of information technology to gain an illegal or an unauthorized access to a computer system with intent of damaging, deleting or altering data.

The fraud in E-Banking sector is covered under the types of cyber-deception. Cyber-deception is further defined as an immoral activity which includes theft, credit card fraud, and intellectual property violations. Mostly frauds are committed because of two goals, one to gain access to the user's account and steal his personal information and transfer funds from one account to another account. Second is to undermine the image of the bank and block the server because so that the customers is unable to access his account.

The following are some types of fraud are taking places in the recent; these frauds mostly are performed by internet. Internet banking frauds or scams victims mostly, those customers who are an innocent customers and poor user of E-banking and they easily believe on banks and their personnel. Mainly internet banking fraud is targeted on dormant account (sleeping account holder).

Cyber crime related with banking sector

- Phishing
- Credit card fraud
- Hacking
- Spyware
- Spam
- Card Skimming
- ATM Skimming
- A identity theft
- EFTPOS Skimming

Phishing: A person's personal details are obtained by fraudsters posing as bankers, who float a site similar to that of the person's bank. They are asked to provide all personal information about themselves and their account to the bank on the pretext of database up gradation. The number and password are then used to carry out transactions on their behalf without their knowledge. In short Phishing involves using a form of spam to fraudulently gain access to people's online banking details.

Credit card fraud: Many online credit card fraud are made when a customer use credit card or debit card for any online payment, a person who had a criminal intention use such card detail and password by hacking and make misuses of it for online purchase for which the customers card used or hacked is injured for such kind of attract or action of a fraud made by and evil. The hacker can misuse the credit card by impersonating the credit card owner when electronic transactions are not secured.

Hacking: Hacking is a crime. Hacking is an attempt to exploit a computer system or a private

network inside a computer. Simply put, it is unauthorized access to or control over computer network security system for some illicit purpose, by hacking the banking sites or accounts of the customers. Hacking is not defined in the amended IT Act, 2000. But under section 43(a) read with section 66 of information technology (Amendment) Act, 2008 and under section 379 & 406 of Indian Penal Code, 1860 a hacker can be punished.

Spyware: Spyware is unwanted software that infiltrates your computer device, stealing your internet usage data and sensitive information. It is the number one way that online banking credentials are stolen and used for fraudulent activities.

Spam: Spam is an electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary but are essentially commercial and often annoying their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.

Card Skimming: Skimming is an illegal practice used by identity thieves to capture credit or debit card information from a cardholder surreptitiously. It can occur at any bank ATM or via a compromised EFTPOS machine. Captured card and PIN details are encoded onto a counterfeit card and used to make fraudulent account withdrawals and transactions.

ATM Skimming: fraudsters can attach false casing and PIN pad overlay onto genuine existing ATMs, or they can attach a camouflaged skimming device onto a card reader entry used in tandem with a concealed camera to capture and record PIN entry details.

A identity theft: A large number of identity theft crimes occur over the internet. Criminals can get a hold of your personal information through your computer and then set up fake bank account or take put loans in your name

CHAPTER III

E-Banking Laws in India and Fraud Risk Management

India is a signatory of WTO. The basic principles of WTO are Liberalization, Globalization and

Privatization. Therefore, Trade and commerce in India has been liberalized. Incidentally, the financial sector has also undergone major changes. With the advent of E- banking, India is facing unprecedented competition from the World at large. If technology is not updated in financial sector, international trade would be a distant dream.⁵

The legal framework of the Indian Banking System is governed by the following set of statutes which are as follows:

- *The Banking Regulation Act, 1949*
- *The Reserve Bank of India (RBI) Act, 1934*
- *Foreign Exchange Management Act 1999*
- *Indian Evidence Act, 1872*
- *Indian Contract Act, 1872*
- *Information and Technology (IT) Act, 2000*
- *Securitization and Reconstruction of Financial Assets and Enforcement of security Interest (SARFAESI) Act, 2002*
- *Negotiable Instruments Act, 1881*
- *Indian Penal Code, 1860*

Provisions of Information and Technology Act, 2000- This Act, extensively deals regarding the Management in offering E- Banking Services by the Bank Channels along –with dealing to specific provisions for curbing Cyber Crimes.

Provisions of Indian Penal Code, 1860 – The main provisions to dealing with the E-Banking

⁵ <http://jsslawcollege.in/wp-content/uploads/2013/05/LAW-RELATING-TO-E-BANKING-IN-INDIA-AN-OUTREACH-CHALLENGE.pdf>

frauds in India are as follows:

- Section 383: Punishment of Extortion
- Section 379: Punishment of theft
- Section 406: punishment of Criminal Breach of Trust
- Section 417: Punishment of Cheating
- Section 471: Using as genuine a forged document or electronic record
- Section 506: Punishment of Criminal Intimidation

Fraud Risk Management: there is a need for a proper and consolidated fraud governance standard. The fraud risk management and fraud investigation must be owned by the banks itself. Banks in India shifted to core banking business and have moved transactions to payments through the electronic channels like ATMs, internet banking mobile banking etc. Fraudsters have also playing an active role as customer into this electronic world banking. The response of the banks related the fraud needed further improvements to overcome through the E-banking fraud easily.⁶

The following are the some important ways of fraud risk management.

1. A strong KYC (know your customer) process is the backbone of fraud prevention activity. Physical securitize of documents of old customers and as well as of new customers also.
2. In every bank must have created a proper training, workshop or mechanism for employee about the various types of fraud and how to detect the frauds and their prevention ways.
3. Banks can have purposeful email IDs or mobile number for customers to reply any

⁶ E-BANKING FRAUDS AND FRAUD RISK MANAGEMENT Tactful Management Research Journal
ISSN:2319-7943

fraudulent activity that they may notice. A devoted team for to reply to customers queries and concerns through the above email IDs. Bank head office to make sure that replying all queries as soon as possible done by that team or not.

4. Every banking institute must have and maintain the capable and strong “Transaction Monitoring Team”. The character of this team is to keep view on transaction taking place whether any incredulous transaction is going out or not as per the banking norms. If they found any suspicious transactions then they take necessary action against that account holder, and investigation.
5. “Precaution is better than cure” create a team known as “Fraud Prevention Team” work of this team is to keep trace out the fraud activity and prevent that from fraud before it actually performed.
6. All banks must have independent division to regulate frauds, their role is monitoring, investigation, reporting and of course mainly run the awareness programs/camps for customers as well as employee also.

CHAPTER VI

RBI role in the legal and security concerns in banking sector

The Reserve Bank of India has issued many circular to Internet Banking. The Reserve Bank of India as a supervisor will cover the entire risks associated with electronic banking as a part of its regular duty. It is the statutory duty on every bank that they should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customer. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.⁷

SUGGESTION AND MEASURES:

The Banking System is the backbone of a Country and its Economy; therefore after analyzing the

⁷ RBI Vide Circular DBOD.AML.BC. no. 11/14.01.001/2012-13

above matter most of the Banks have already implemented the E-Banking Facilities, as these facilities are beneficial to both i.e. banks as well as customers. The banks are facing many challenges about fraudulent activities, threat, work load on their employee etc. with all the issues Banks and financial institutions are bound to serve a safe banking, for the safe banking practice some suggestions and measures in this reference are as follows:

- For better protection the account holders create a strong password, secure the computer/ mobile device and check into up to date, monitoring the accounts regularly.
- Each bank should incorporate one In-House Cyber Grievance Redressal Cell, who could directly deal with the banking frauds happening in their banks, they must analyze their functions and affairs annually and send their annual Report to the concerned State Cyber Cell or The District Cyber Cell for their expert advice and guidance.
- Banks are under obligation to maintain secrecy of customers account.⁸

CONCLUSION:

Technology is always a double-edged sword can be used for both purpose, good or bad. As electronic payments volumes increase day by day, and today scenario banking exercise boost by web and mobile devices, the capacity to find and prevent cyber crime (fraud) and dwindle that frauds has become critical. The burden on financial institutions is to protect their customers from fraud, protect themselves from losses due to financial / cyber crimes. Preamble of IT Act 2000 provides that the Act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce. Further the Act also made amendments to the IPC 1860, Indian Evidence Act 1872, The Bankers Book of Evidence Act 1891, and the Reserve Bank of India 1934 for expedite legal recognition and regulation of the commercial activities. The law makers have to go the extra mile compared to the fraudsters, to keep them at bay. The legal issues of internet banking / e-banking in India must be taken more seriously by all stakeholders especially the Indian Banks. However, better result cannot

⁸ Section 13 of *Banking companies (Acquisition and transfer of Undertaking) Act, 1970*

be achieved till laws about e-transaction or there frauds more strictly and implement by authorities and cyber security requirements made mandatory on the part of Indian Banks.