Internet Banking: Legal and Security Issues Vis a Vis Regulatory Framework in India

A Dissertation Submitted

To

Sikkim University

In Partial Fulfilment of the Requirement for the

Degree of Master of Philosophy

By

Amar Bhandari

Department of Law

School of Social Sciences

February 2017

DECLARATION

Date: .....

I declare that the dissertation entitled **"Internet Banking: Legal and Security Issues Vis a Vis Regulatory Framework in India"** submitted to Sikkim University for the award of the degree of **Masters of Philosophy in Law** is my original work. This dissertation has not been submitted for any other degree of this University or any other university.

Amar Bhandari
M.Phil Scholar
Roll No: 15MPLW02
Registration No: 15/M.Phil/LAW/04
Department of Law
Sikkim University
Tadong-737102

We recommend that this dissertation is placed before the examiners for evaluations.

Name of the Chairperson

Prof. Imtiaz Gulam Ahmed

(Head) Department of Law

Sikkim University

Name of the Supervisor

Dr. Nidhi Saxena

Assistant Professor

Department of Law

Sikkim University

CERTIFICATE

This is to certify that the dissertation entitled "**Internet Banking: Legal and Security Issues Vis a Vis Regulatory Framework in India"** submitted to the Sikkim University in partial fulfilment for the requirement of the degree of **Masters of Philosophy in Law** is embodies the results of the bonafide research work carried out by **Mr. Amar Bhandari** under my guidance and supervision.

All the assistance and help received during the course of investigation have been duly acknowledged by him.

Supervisor:

Dr. Nidhi Saxena

Assistant Professor
Department of law
Sikkim University
Tadong- 737102

Place: _____

Date: _____

PLAGIARISM CHECK CERTIFICATE

This is to certify that plagiarism check has been carried out for the following M.Phil dissertation with the help of *Urkund* software and the result is within the permissible limit decided by the University.

Internet Banking: Legal and Security Issues Vis a Vis Regulatory Framework in India

Submitted by **Mr. Amar Bhandari** under the supervision of

Dr. Nidhi Saxena, Assistant Professor, Department of Law,
School of Social Sciences, Sikkim University,
Gangtok-737102, India

Signature of the Candidate

Countersigned by the Supervisor

ACKNOWLEDGEMENT

First of all, I am grateful to The Almighty God for establishing me to complete this dissertation.

I would like to express my sincere gratitude to Prof. (Dr.) Imtiaz Gulam Ahmed (Head of Department), Department of Law (Sikkim University), for his constant encouragement. I place on record, my sincere gratitude to my supervisor Dr. Nidhi Saxena, I am extremely grateful and indebted for her expert, sincere and valuable guidance and encouragement extended to me.

I take this opportunity to record my sincere thanks to all the faculty members of the Department of Law (Sikkim University) for their help and encouragement. I am thankful to the Library Staffs for helping me provide the references for present work and other academic pursuits.

I am thankful to my cousin brother Mr. Pravakar Rai for his support. I acknowledge my eternal gratitude to my mother and father on whom I owe everything I have and have yet to achieve. I would like to express my deepest gratitude to my friends Mr. Libron Wangchuk Rongong, Mahendra Thapa and Mr. Anxa Limboo for their help and encouragement.

I would like to give my special thanks to University Grant Commission (UGC) for providing me the finance for undertaking this research project.

What are collected in this dissertation paper are materials that I found in Articles, Books, Journals or Internet. I make no claim to be comprehensive. A special thanks to the authors mentioned in the references page.

I also place on record, my sense of gratitude to one and all who, directly or indirectly, have lent their helping hand in this venture.

Thank You

Amar Bhandari

CONTENT

		Page No.
	DECLARATION	i
	CERTIFICATE	ii
	PLAGIARISM CHECK CERTIFICATE	iii
	ACKNOWLEDGEMENT	iv
	CONTENT	v-vii
	ABBREVIATION	viii-ix
CHAPTER- I		1-16
1.	INTRODUCTION	1
1.1.	CONCEPT OF INTERNET BANKING	9
1.2.	GROWTH OF INTERNET BANKING	10
1.2.1.	COMPETITION	10
1.2.2.	COST EFFICIENCIES	10
1.2.3.	GEOGRAPHICAL REACH	11
1.2.4.	CUSTOMER DEMOGRAPHICS	11
1.2.5.	DIGITAL INDIA PROGRAMME	11
1.3.	RESEARCH OBJECTIVES	14
1.4.	RESEARCH QUESTIONS	14
1.5.	HYPOTHESIS	15
1.6.	RESEARCH METHODOLOGY	15
1.7.	CHAPTERIZATION	15
CHAPTER-II		**17- 31**
2.	EXISTING ARCHITECTURE OF INTERNET BANKING IN INDIA	17
2.1.	PRESENT SCENARIO OF INTERNET BANKING IN INDIA	19
2.1.1.	ELECTRONIC BILL PAYMENT	21
2.1.2.	AUTOMATED TELLER MACHINE	21
2.1.3.	ELECTRONIC CLEARING SERVICES	22
2.1.4.	ELECTRONIC FUND TRANSFER	24
2.1.5.	ACCOUNT OPENING REQUEST	25

2.1.6.	ACCOUNT STATEMENT	25
2.1.7.	TRANSACTIONS ENQUIRY	26
2.2.	PRE-LOGIN SECURITY AND PRIVACY FEATURES	28
2.3.	POST-LOGIN SECURITY AND PRIVACY FEATURES	30
CHAPTER-III		**32-52**
3.	A COMPARATIVE OVERVIEW OF INTERNET BANKING SERVICES IN VARIOUS COUNTRIES	32
3.1.	USA	33
3.1.1.	ONLINE BANKING: THE EARLY YEARS	33
3.1.2.	ONLINE BANKING IN THE 2000S	35
3.1.3.	POSITION OF REGULATORY FRAMEWORK OF INTERNET BANKING IN USA	37
3.2.	U.K.	43
3.2.1.	POSITION OF REGULATORY FRAMEWORK OF INTERNET BANKING IN UK	44
3.3.	AUSTRALIA	47
3.4.	INDIA	49
CHAPTER-IV		**53-64**
4.	ISSUE OF INTERNET BANKING.	53
4.1.	PROBLEM RELATING TO ONLINE OPENING OF ACCOUNT	54
4.2.	PROBLEM OF AUTHENTICATION AS WELL AS BANKS IN INDIA LAG IN SECURITY OF CARD TRANSACTIONS	54
4.3.	LIABILITY OF BANKS IN BILATERAL AGREEMENT	58
4.4.	PROBLEM RELATING TO PRIVACY AND CONFIDENTIALITY OF CUSTOMERS ACCOUNT AND INADEQUACY OF DATA PROTECTION LAW	59
4.5.	CYBER SECURITY OF BANKS IN INDIA NEEDS STRENGTHENING	62

CHAPTER-V **65-97**

5. LEGAL FRAMEWORK OF INTERNET BANKING IN INDIA 65

5.1. MODAL LAW IN INTERNET BANKING 68

5.2. BANKING SERVICES 72

5.2.1. RESERVE BANK OF INDIA ACT, 1934 73

5.2.2. BANKING REGULATION ACT, 1948 75

5.2.3. INFORMATION TECHNOLOGY ACT, 2000 77

5.2.4. RBI GUIDELINES ON INTERNET BANKING. 80

CHAPTER-VI **98-124**

6. CONTRIBUTION OF JUDICIARY IN INTERNET BANKING 98

CHAPTER-VII **125-138**

7. CONCLUSION AND SUGGESTIONS. 125

7.1. SUGGESTIONS 137

REFERENCES **139-145**

ABBREVIATION

ATM	Automated Teller Machines
ASIC	Australian Securities and Investment Commission
CEO	Chief Executive Officers
CHIPS	Clearing House Interbank Payment System
CNP	Card Not Present
CVV	Card Verification Value
CVVC	Card Verification Value Code
DBSB	Development Bank of Singapore Bank.
DTMF	Dual Tone Multi Frequency
DSS	Decision Support System
DoS	Denial of Service
DDoS	Distributed Denial of Services
DoT	Department of Telecommunications
DBOS	Department of Banking Operation and Development
EBPP	Electronic Bill Presentment and Payment
ECC	Electronic Clearing Cards
ECHR	European Commission on Human Rights
EFT	Electronic Fund Transfer
ECS	Electronic Clearing Services
EFTPOS	Electronic Fund Transfer Point & Sale
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institution Technology
FRB	Federal Reserve Board
FRS	Federal Reserve System
GLB	Gramm-Leach-Bliley
HDFC	Housing Development Finance Corporatio
HTML	Hyper Text Markup Language
HSBC	Hongkong and Shanghai Banking Corporation
IS	Information System
IT	Information Technology

IMF	International Monetary Fund
ICICI	Industrial Credit and Investment Corporation
IIM	Indian Institutes of Management
IDRBT	Institute for Development & Research in Banking Technology
IP	Internet Protocol
KYC	Know Your Customers
MIS	Management Information System
NBS	Nottingham Building Society
NCUA	National Credit Union Association
NEFT	National Electronic Fund Transfers
OCC	Office of the Comptroller of Currency
OTS	Office of Thrift Supervision
PIN	Personal Identification Number
RBI	Reserve Bank of India
RFID	Radio Frequency Identification
RTGS	Real Time Gross Settlement
SFNB	Security First Network Bank
SHP	Safe Harbour Principles
SIP	Systematic Investment plan
SMS	Short Message Service
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunications
UCC	Uniform Commercial Code
UETA	Uniform Electronic Transaction Act
UK	United Kingdom
UNCITRAL	United Nations Commission on International Trade Law
URL	Uniform Resource Locators
URSIT	Uniform Rating System for Information Technology
USA	United State of America

CHAPTER I

1. INTRODUCTION

Banking is the backbone of an economy, because an economy totally depends upon the banking. The emergence of online banking has marked the end of traditional banking era. In this new age of technology and internet people can connect to other part of the world with just a click of a button. The facility of online banking has made the day to day living more convenient as they do not have to stand in bank for hours. However, the intangible nature of online transactions creates fear among common people and affects the willingness of customers to engage in online activity. Thus, the acceptance of online transactions system totally depends upon the user's trust. So before going into detail on the online banking it is better to have an overview of its origins. Information technology (IT) is the acquisition, processing, storage and dissemination of vocal, symbolic, textual and numerical information by a micro electronics - based combination of computing and telecommunications. IT (information technology) is a term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived)[1]. It is the technology that is driving what has often been called "the information revolution." IT (Information Technology) is the area of managing technology and covers wide variety of areas that include but they are not limited to things such as processes, information systems, computer software,

[1] "Final Study of Internet Banking in India", online available at http://www.slideshare.net/Dharmikpatel7992/final-study-of-internet-banking-in-india-24278173, accessed on 25 of oct. 2016., at 4:45p.m.

programming languages, computer hardware and data constructs. In short, Information Technology is anything that renders data, information or perceived knowledge in any visual format whatsoever, via any multimedia distribution mechanism. IT provides businesses with four sets of core services to help execute the business strategy and these four core services are broken into business process automation, connecting with customers, providing information, and productivity tools. IT professionals execute a variety of tasks (IT Disciplines/Competencies) that ranges from installing applications to designing complex computer networks and information databases and some of these duties are data management, engineering computer hardware, networking, database and software design, as well as supervision and administration of whole systems. Information technology is starting to spread further than the conventional personal computer and network technologies, and more into integrations of other technologies such as the use of cell phones, televisions, automobiles, and more, which are increasing the demand for such jobs[2].

Many of the largest banks in the world emerged successful from the technical changes as they are able to recognize at an early stage. Whereas India's banking sector has a long way to go before it can compete globally due to the late introduction of ICT in Indian banks. Indian bank should be equipped with the latest technology and adapt to its surrounding to provide and update information to increase productivity which further leads to a competitive advantage. However it should be customer- friendly, efficient and competitive in the current authorities and businesses. They also need the technology to newer products and newer forms of service and the increasingly dynamic global environment to offer. Information technology allows banks to build

[2] Ibid.

new systems, which bite the needs of many customers that cannot be considered today. In internet banking, for example, it allows customers to conduct their banking transactions in a direct access to the core of the bank customer account works, but they should verify all the information. In the future, the banks can free all the constraints of a delivery channel. They can also create, package, market and product niches, because of the tumbling price of the technology, they can do so cost-effectively. Technology gives banks the opportunity to be closer to customers, to a broader range of services at lower costs, and streamline the systems so that all information can be used for the trends that can quickly lead into new products. Electronic banking data can be gathered and analyzed. Internet banking refers any customer with a computer and an internet connection can get connected to his banks website to do any of the virtual banking functions. Every service that the bank has permitted on the internet is show in the banks website. Any service can be selected and further interaction is dictated by the nature of service. Just the once the branch offices of bank are organized with internet, the identity of any branch would be borderless entity and which permit the banking services at anytime and anywhere. Internet banking is a generic term making use of electronic channels through telephone, mobile, internet etc. for delivery of banking services and products. India is still in the early stages of internet banking growth and development. "Internet banking means a lot more than just going paperless, leading banks are offering a new, improved and better customer experience and delivering faster and more efficient services."[3] Information Technology has become one of the most important and necessary tool in today's organizations. Banks today operate in a highly globalized, liberalized, privatized and a competitive

[3] "Banking in Digital World", source available at http://www.atkerney.de/documents/856314/3998533/Banking+in+a+digital+world.pdf. Accessed on 12/04/2016 at 7:45 p.m.

environment. In order to withstand in this environment banks have to use Information Technology. Information technology has introduced new business paradigm. It is increasingly playing a significant role in development of banking industry. There are a variety of ways to approach internet banking. For leading banks, there are mainly four interconnected, mutually reinforcing elements: connectivity, automation, innovation, and decisioning. Connectivity refers to how can banks use rapidly growing social networks to build loyalty and competition-disrupting offerings. Automation refers to how to harness digitalization in process re-design for a better customer experience and more effective use of resources. Innovation refers to how banks should continue to renew themselves, given the rapid pace of change in the industry. Decisioning refers to how big data can be used to make better, faster, and more accurate decisions regarding customer purchase choices as well as banks' decisions on issues such as risk.[4] Moreover, Internet banking is called online banking for all financial transactions, because it includes the source of features such as obtaining information, transferring money, and purchasing goods and expert services in an online environment. These days, the Internet is used as a main channel for financial activities.

It has been forecast by many that online banking will continue to be the most popular and fastest method for future electronic financial transactions. For instance if a customer wants to Withdrawal: the cardholder can withdraw funds from their account, from an ATM machine. In ATM Deposit: Cardholders can deposits funds to their account (typically at an ATM). In Inter-account transfer: it allows transferring funds

[4] Deepshika Jamwal & Devanand Padha, *"Internet Banking System in India: Analysis of Security Issue",* (February 26-27, 2009), online available at http://www.bvicam.ac.in/news/INDIACom%202009%20Proceedings/pdfs/papers/80.pdf, accessed on 14/06/2016 at 8:41 a.m.

between linked accounts belonging to the same cardholder. In Inquiry: a transaction without financial impact, for instance balance inquiry, available funds inquiry or request for a statement of recent transactions on the account Administrative, this covers a variety of non-financial transactions including Personal Identification Number (PIN) change EFT transactions require authorisation and a method to authenticate the card and the card holder. Whereas a merchant may manually verify the card holder's signature, EFT transactions require the card holder's PIN to be sent online in an encrypted form for validation by the card issuer. Other information may be included in the transaction, some of which is not visible to the card holder (for instance magnetic stripe data), and some of which may be requested from the card holder (for instance the card holder's address or the CVV2 security value printed on the card).

Internet Banking permits consumers to perform banking business through protected link activated by their financial institution. Internet banking is very beneficial and advantageous for banks and their clients. As it include cost savings, time savings, achieving new segments of the society, effectiveness, improvement of the bank’s status and better customer service and client satisfaction. Since internet banking has the intangible nature, clients can only become motivated through trust, as it plays an important role in improving the level of the availability of Internet banking in the online environment. It is widely recognised that internet banking provides more revenue per customer and costs less per transaction. In contrast with offline banking, the concept of trust is a vital consideration in online banking because the customers involved in the financial activities are concerned about sharing the essential files and important information through the Internet.

The revolution in the banking sector "has been largely brought about by liberalization and economic reforms that allowed banks to explore new business opportunities rather than generating revenues from conventional streams"[5] of borrowing and lending. The reforms brought the environment for the banking sector. Now a days, to provide banking products and services the banks are providing machinery based multi delivery channels. "Based on the recommendations of these committees and working groups, the Reserve Bank issued suitable guidelines for the banks. In the 1980s, usage of technology for the back office operations of the banks predominated the scene"[6]. For automation and mechanization in the financial sector a high level committee was set up under the chairmanship of *Dr. C. Rangarajan*. And the committee introduced a plan for automation to other areas like Email, ATNs etc.

As modern banking increasingly relies on the internet and computer technology to operate their businesses and market interactions, the threats and security breaches are highly increase in recent years.

So internet banking presents challenges to financial security and personal privacy when banks information is compromised by skilled criminal hackers by manipulating a financial institutions online information system. This causes huge financial losses to the banks customers.

---

[5] Boby Johl & others, "Quality and Realiability Engenerring: Recent Trands and Future Directions" , available at https://books.google.co.in/books?id=dsTXCQAAQBAJ&pg=PA163&lpg=PA163&dq=has+been+largely+brought+about+by+liberalization+and+economic+reforms+that+allowed+banks+to+explore+new+business+opportunities+rather+than+generating+revenues+from+conventional&source=bl&ots=0Tnrdzom2d&sig=MobL9ECmwYxHGYSMFjbTDCa4RE&hl=en&sa=X&ved=0ahUKEwiV47Cep_3RAhUEuI8KHbTqBOAQ6AEIIDAB#v=onepage&q=has%20been%20largely%20brought%20about%20by%20liberalization%20and%20economic%20reforms%20that%20allowed%20banks%20to%20explore%20new%20business%20opportunities%20rather%20than%20generating%20revenues%20from%20conventional&f=false, accessed on 7th Feb. 2017 at 11:36 a.m.

[6] Goel,Manjusha, "Impact of Technology on Banking Sector in India"', available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.676.7006&rep=rep1&type=pdf , accessed on 07/02/2017.

Banks information is compromised by skilled criminal hackers by manipulating a financial institution's online information system, spreading malicious bank Trojan viruses, corrupt data, and impede the quality of an information system's performance…so at present customers can do banking online which is easy and time saving and at the same time they are vulnerable to threats.[7] So one of the major concerns of people with respect to internet banking is the safety related to data of bank accounts, transactional information and also the access path of their account.[8]

The new concept is Financial Inclusion: Recent developments in Information technology has transformed banking from the traditional brick-and-mortar model to sleek, easy and Anytime, Anyhow, Anywhere banking supported by a number of innovative systems such as Automated Teller Machines (ATM), cashless banking through plastic money, Internet Banking, mobile banking, online money transfers, etc. But technology is expensive and, therefore, is till now restricted to urban population who can afford its cost. Whatever has so far reached to rural population is meagre, to say the least. In the new millennium, India has witnessed tremendous growth in communication technology.[9] Notwithstanding the global meltdown in the last couple of years, this sector has grown tremendously with the result that now communication has made inroad in urban and semi urban areas and is set to cover more and more new areas. With such expansion, it has also become affordable. With this growth, a new

[7] Zakaria Karim, Mohammed Rezaul, Aliar Hossain*, "towards Secure Information System in Online Banking".*

[8] Internet banking in india, source available at http://tips.thinkrupee.com/articles/internet-banking-in-india-php.

[9] Ibid.

channel of reaching the masses has opened up.[10] Security extends from the bank's hardware to the user's device – whether a PC/Mac at home, an iPad or the newest Smartphone. In all cases, internet banking must employ robust security technologies which protect the communication, user information and the bank's IT infrastructure.[11]

Indeed, it is clear that for internet banking to be a rewarding experience for the customer and a profitable growth area for the banks, technology partners, mobile phone operators and payment processing service providers – there ought to be a inclusive agreement on shared technology standards and processes. The European Commission has just issued a Green Paper, 'Towards an integrated European market for card, internet and mobile payments' which addresses many of the issues while being much broader than online banking itself[12].

Reserve Bank of India (RBI) that is the Banker's Bank so they have a duty to issue appropriate directions for bank operation and they has been issuing various directions and recommendations from time to time to strengthen cyber security banks operating in India. However, RBI observed that at present some banks do not have proper security policy and methods to monitor the service level agreement with third parties and have inadequate audit trail, so it has issued warning to banks to comply the directions of RBI by Oct, 2012 and June 30, 2013. Further internet banking becomes less secure if users are computer illiterate. An increasingly popular criminal practice is to gain access to a user's finances through phishing and other threats Malware,

[10] Online available at http://www.syndicatebank.in/scripts/financialinclusion.aspx, accessed on 13/06/2016 at 9:20 p.m.

[11] Supra note 4.

[12] Vincent Villers, *"Banking will mean digital banking in 2015",* Press releases on jan. 2015, online available at http://www.pwc.lu/en/press-articles/2012/banking-will-mean-digital-banking-in-2015.html, accessed on 25/04/2016 at 7:26p.m

Viruses, theft of user identity and password through other means etc. Therefore, if the people want to use online banking to conduct financial transactions, they should make themselves aware of the risks and take precautions to prevent and minimize them.

1.1. CONCEPT OF INTERNET BANKING

The technology that has been widely adopted by consumers has powerful capabilities including greater bandwidth, advanced data security, and stronger privacy protection that offer new opportunities for the banks. In the world of banking, the development of information technology has a large effect on development of more flexible payment methods and more-user friendly banking services.

Internet Banking is a product of e-commerce in the field of banking and financial services. In what can be describe as Business – to – Consumer (B2C) domain for banking industry, Internet banking offers much more different online services like balance enquiry, request for cheque books, recording stop payment instruction, balance transfer instruction, account opening and other forms of traditional banking services. Online banking is also known as "internet banking" or "web banking." An online bank offers customers just about every service traditionally available through a local branch, including deposits, which is done through the mail, and online bill payment.

The Definition of Internet Banking: "We can set Internet banking as a set of technological tools that offers a financial institution for its customers to make banking transactions via the computer using our Internet connection." The Internet banking service is based upon a connection that integrates the functionalities of a bank branch.

1.2. GROWTH IN INTERNET BANKING

The competitive charge, customer facility, and demographic concerns etc are the main reason to appealing the banks to access the technology and internet banking policies. Last 20 years are witnessing the acceptance of Internet throughout the country, people are more comfortable in doing banking through internet. There are serial reasons for this acceptance like-

1.2.1. COMPETITION:

The competitive pressure from several banks is the most important cause behind the growing use of internet banking technology. Some others reasons like cost reduction and revenue enhancement is ranking second and third place respectively.

1.2.2. COST EFFICIENCIES:

One of the reasons behind the growth of Internet Banking is cost efficiency. The delivery costs of Internet banking services are lower than customary banks. The real expenses to carry out a business will vary depending on the delivery way used. Banks are likely to decrease these costs endlessly.[13] Banks were improving their technologies continuously for providing banking product and services by the mainly cost-effective way.

[13] Gunajit Sarma & Pranav Kumar Singh, *"Internet Banking: Risk Analysis and Applicability of Biometric Technologies for Authentication",* 69 (International Journal of Pure and Applied Science and Technology), 1(2) (2010), online available at https://pdfs.semanticscholar.org/3b10/0fe0af708daf4457c17de0ffcfcad4d07cc4.pdf

1.2.3. GEOGRAPHICAL REACH:

Geographical distance reduces access to bank in the same way internet obliterate the distance. Hence internet banking brings it within the reach of public. There are some banks offering services through internet while there are some banks businesses through internet only, without having any traditional banking offices. Actually some banks are doing their business through internet only, they have no traditional banking offices and they reach their customer via the internet. Internet banking transactions are performed by customers from any part the country. And some of the financial institutions are doing their business through traditional banking offices with using the Internet as an alternative delivery channel.

1.2.4. CUSTOMER DEMOGRAPHICS:

The different banking customers' demands for different service accordingly Internet banking permits banks to present a broad range of choice in their services. A number of customers will depend on traditional branches to conduct their banking transactions. They are believed traditional way of doing banking transaction is the most secure in comparison to internet banking, while some are comfortable new technologies that arrive in the marketplace to do their banking business.

1.2.5. DIGITAL INDIA PROGRAMME:

In India the E-governance initiatives was initiated in the mid 1990s with emphasis on citizen-centric services. Some major projects such as railway computerization, land record computerization, etc. are the major ICT initiatives of the Government, which

focused mainly on the development of information systems[14]. Later on the national level e-Governance programme called National e-Governance Plan was initiated in 2006. Under this Plan there were 31 Mission Mode Projects covering a wide range of domains, viz. agriculture, land records, health, education, passports, police, courts, municipalities, commercial taxes, treasuries etc.

There were 31 Mission Mode Projects under National e-Governance Plan covering a wide range of domains, viz. agriculture, land records, health, education, passports, police, courts, municipalities, commercial taxes, treasuries etc. 24 Mission Mode Projects have been implemented and started delivering either full or partial range of envisaged services. The portfolio of Mission Mode Projects has increased from 31 to 44 MMPs. Many new social sector projects namely Women and Child Development, Social Benefits, Financial Inclusion, Urban Governance, e-Bhasha…etc have been added as new MMPs under e-Kranti[15].

Prime Minister *Narendra Modi* lunched the Digital India Programme on 1st July 2015, with an aim to connect rural areas with high-speed internet network. This programme consist of three main Digital India consist of three core components i.e. digital infrastructure as a core utility to every citizen, governance and services on demand, digital empowerment of citizens[16]. *Pradhan Mantri Jan-DhanYojana (PMJDY)* and digital India schemes encourage rural people to online banking services, which play a crucial role in growth of banking sector in India. To implement this mission in banking

[14] Online available at digitalindia.gov.in/content/introduction.

[15] "Digital India: Opportunities Beyond Imagination", online available at mobilityindia.com accessed on 29th Nov. 2016.

[16] "India is first country to give discounts on online payment", online available at www.daytodaygk.com accessed on 29th Nov. 2016.

sector, on 8t-h November 2016 by our Prime Minister *Narendra Modi* has announced that the demonetisation of 500 and 1000 rupee note. Now India is going through demonetisation, a major aim of which is to promote digital transactions. India continues to be driven by the use of cash; less than 5% of all payments happen electronically, however the finance minister, in 2016 budget speech, talked about the idea of making India a cashless society, with the aim of curbing the flow of black money. Even the RBI has also recently unveiled a document- "Payments and Settlement Systems in India: Vision 2018"- setting out a plan to encourage electronic payments and to enable India to move towards a cashless society or economy in the medium and long term.

The legal framework for banking in India is provided by a set of enactment, viz., the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934, and the Foreign Exchange Management Act, 1999. Broadly, without obtaining a license from Reserve Bank of India no entity can functions as a banks in India. Different types of activities which a bank may undertake and other prudential requirements are provided under this Act. Acceptance 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. Beside 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, Bankers Books Evidence Act, 1891, etc.[17] Internet banking is an extension of the traditional banking,

[17] M.L.Tannan, Tannan's, "*Banking Law and Practice in India"*, (20th Ed.), (New Delhi: India Law House, 2003), p.157

banks uses internet as a medium for delivering banking services and also receiving instructions from the customers. Therefore, various provision of law, which are applicable to traditional banking activities, is also applicable to internet banking. Apart from these the Indian Government passed Information Technology Act in 2000 for the protection of cyber crime and also the RBI provides many guidelines for Internet banking.

1.3. RESEARCH OBJECTIVES

The research aims at enriching the knowledge and understanding of Internet Banking: security and privacy issues and its regulatory framework in India. Specifically the main objectives of this study are:

1. To study about the existing architecture of Internet Banking in India.
2. To know about the various security and legal issues coming up in internet banking as well as the latest technical and legal solution adopted by banks to handle them.
3. To know about the various legal framework of Internet banking services in India.
4. To study about the various internet banking laws and guidelines issued by RBI and other regulatory authority and whether banks are followed this guidelines or not.
5. To analyze the contribution of judiciary in regulating i-banking services

1.4. RESEARCH QUESTIONS

1. What is the existing architecture of Internet banking in India?
2. What are the various security and legal issues coming up in internet banking as well as what the latest technical and legal solution adopted by banks to handle them?

3. What is the legal framework of Internet banking services in India and to what extent they are accommodating these issues?
4. How far RBI guidelines are helping to handle these very issues in banking sector?

1.5. HYPOTHESIS

"**In internet banking there are various legal & security issues but the regulatory framework to deal with is very weak.**"

1.6. RESEARCH METHODOLOGY

This research paper is based on secondary resources. In order to achieve the objective i.e. the extent of Issues in Internet Banking, the researcher have collected the data related to Internet Banking from the different banks. Hence the research is totally based on doctrinal data. In order to understand the trend, researcher have also gathered some other secondary data from other sources like government, research papers periodicals, journals, authentic websites (official, private), published reports of Internet Banking etc. The researcher has also examined the court decision taken on the various issues of banking services as well as internet banking.

1.7. CHAPTERIZATION

1. Introduction

   This chapter gives an overview of the nature of study, concept, advantages and disadvantages of internet banking. And also gives the reason for growth of internet banking.

2. Existing Architecture of Internet Banking In India

   This chapter will study about the existing architecture of internet banking in India and different products and services offered by Indian as well as foreign banks in India. And also this examined about the cyber fraud protection features provided by banks.

3. A Comparative Overview of Internet Banking services in some Countries.

   This chapter will examined the development of internet banking in different countries and also study about the Act of legislation of these countries.

4. Issues of Internet Banking

   This chapter will examined about the various legal and security issues of internet banking in India.

5. Legal Framework of Banking Services

   This chapter will study about the various Act of Legislations as well as RBI guidelines which are passed for the regulation of internet banking in India.

6. Contribution of Judiciary in Internet Banking

   This chapter will examined about the various judicial decision of different courts in India.

7. Conclusion and Suggestions.

   This chapter will conclude all the chapters in brief and also provide the finding of the study as well as give some suggestions also.

CHAPTER II

2. EXISTING ARCHITECTURE OF INTERNET BANKING IN INDIA

The Indian banking system has travelled a long path since the independence in1947 from nationalization to liberalization. "It has witnessed transition from a slow business institution to a highly proactive and dynamic entity. This transformation has been brought about by liberalization and economic reforms that allowed banks to explore new business opportunities rather than generating revenues from conventional streams"[18] of barter system. To increase the pace of computerization in the operation of banking sector, Reserve Bank of India was set up high level committees in early 1980s. For the purpose of customer service, two mode of computerization were developed and implement. The first committee introduce computerized section and mechanized sections in the banking sector. And the committee was set up in the year 1988 which introduced a plan for automation to other areas like Email, ATMs, I-Banking etc.

In the last decade, information technology has brought significant changes in the banking sector in way by providing opportunities to the banks for offering differentiated products and services to their customers using innovative technology platforms. Technological transformation undoubtedly changed the policy of bank in service providing in comparison to traditional banks, which were depending on branch to deliver services, have now banks, which were depending on branch to deliver services, via different methods and technology based channels. "All these new

[18] Upadhyay, Dr.Seema Mishra, "A Comparative Study on the Performance of largest Public Sector and Private Sector Banks in India", *IJMSS* Vol.04 Issue-05 (May, 2016) ISSN: 2321-1784, P. 82

channels of distribution are within the domain of e-banking or i-banking.[19] Internet banking has been around for quite some time in the form of automated teller machines (ATMs) and telephone transactions"[20]. As a part of strategic decisions, banks in India have been investing and continued to invest enormous amount of funds on computer and related technologies expecting substantial payoff[21]. The present expenses "on information technology for banks on the whole is Rs 6,500 Cr. per year, about 2.7 per cent of their revenues is further likely to shoot up to Rs 10,000 Cr. annually in the coming years".[22] The infusion of technology in day to day banking business was also emphasised by the Reserve Bank of India

Computerization of banking system was one of the main measures in improving the competence of banking services. The introduction of these reforms brought with it a healthy competition. In order to survive in this competitive environment banks needs to upgrade their customer service to a much higher plane. They found technology as an ideal tool to achieve this objective. Technological aid like ATMs, point of sale devices, smart cards, internet banking and WAP banking has given the customers to chores the channel of getting catered to its requirement.

---

[19] RBI Publication on Operation and Performance of Commercial Bank on 8th Nov. 2012 online available at www.rbi.org.in/scripts/PublicationsView.aspx?id=14629 accessed on 29th Nov. 2016

[20] N. M. Gaikwad & A. U. Rathod, "*Online Banking in India- Advantages & Disadvantages",* Tactful Management Research Journal. Vol. 3 Issue 2, November 2014. P. 1-5.

[21] S. T. Surulivel, C. Vijayabanu, R. Amudha & B. Charumathi, *"Impact of Information Technology (IT) Investments on the Cost Efficiency of Indian Private Sector Banks- A Stochastic Frontier Approach (SFA)".* Research Journal of Applied Sciences, Engineering and Technology, published on 10/08/2013, publish by © Maxwell Scientific Organization, 2013

[22] The Boston Consulting Group (2011)

Traditionally, banks are increasingly relies on branches, branches as a place where banks can render their services such as advising people on their saving or selling them investment products. Now, this system of banking is changing and the changes are more visible in private and foreign banks in India as they perform their functions online and use branches as a core for sourcing loans and providing financial advisory services. To survive with this competitive environment, Indian banks have adopted several initiatives and internet banking is one of them. The competition has been especially tough for the public sector banks as the newly established private and foreign banks are leaders in adoption of internet banking.[23]

2.1. PRESENT SCENARIO OF I-BANKING IN INDIA

"The evolution of internet banking has fundamentally transformed the way banks traditionally conduct their businesses and the ways consumers perform their banking activities".[24] Today internet banking has extraordinary growth and has become one of the major ways for banks to deliver their products and services. Internet banking (i-banking) is defined as the robotic delivery of new and branch banking products and services directly to their customers through internet.[25] Customers access i-banking services using electronic devices. There are various kinds of internet banking services

[23] Deepshika Jamwal and Devanand Padha, *"Internet Banking in India: Analysis of Security Issue",* (February 26-27,2009), online available at http://www.bvicam.ac.in/news/INDIACom%202009%20proceedings/pdfs/papers/so.pdf., accessed on 14/09/2016 at 3:25 p.m.

[24] Ceren Sayar, Simon Wolfe (2007), "*Internet banking market performance: Turkey versus the UK",* International Journal of Bank Marketing, Vol. 25 Iss: 3, pp.122 - 141

[25] Daniel E (1999), *"Provision of electronic banking in the UK and the Republic of Ireland."* International Journal of Bank Marketing 17: 72-82.

which is provided by banks to their customers such as: account balances cheque, transfer funds, electronic bill payments etc.

I-banking offers benefits for both banks and its customers. I-banking has enabled the banks to lower operational costs through the reduction of physical facilities and staffing resources required, reduced waiting times in branches ensuing in potential increase in sales performance and a larger global reach[26]. From the customers' perspective, i-banking provides a wide verity of banking businesses electronically through the bank's website anytime and anywhere. In addition, customers are no longer confined to the opening hours of banks, they do not need to visit bank branches and waiting times are not necessary, and access of information regarding banking services are now easily available through bank's website. Following delivery channels/ services primarily constitute the domain of i-banking are:

2.1.1. Electronic Bill Payment;

2.1.2. Automated Teller Machine

2.1.3. Electronic Clearing Service

2.1.4. Electronic Fund Transfer;

2.1.5. Account Opening Request;

2.1.6. Account Statement;

2.1.7. Transaction Enquiry;

[26] Sarel and Marmorstein, *"Marketing Online Banking Services: The Voice of the Customer",* Journal of Financial Services Marketing, Volume 8, Number 2, 2003

2.1.1. ELECTRONIC BILL PAYMENT

Customers can pay various bill through online directly from his/her account. They can pay their any type of bill such as telephone, electricity, insurance, credit card and other bills from anywhere at any time. By using biller's website customers can buy mutual fund also

The practice of bill payment starts by just logon to banks website with allotted ID followed by registration of the biller to which he wants to pay, with all the bill details. Once the bill is uploaded by the biller, bank can make payment online.

There is also a facility of set up of Auto Pay orders with an upper limit to ensure that our bills are paid automatically whenever they are due.

2.1.2. AUTOMATED TELLER MACHINE

An automated teller machine or automatic teller machine is also known as an automated banking machine, cash machine, cash point, cash line, is an electronic telecommunications device from where customers of a financial institution can perform various task such cash withdrawal, balance enquiry etc. without the need for a human cashier, clerk or bank teller.[27] The automated teller machine is a complicated technology that does not have a single inventor. Instead, the ATMs we use today are contribution of several different inventions. Today's ATMs are stylised computers that can do almost anything a human bank cashier can, and have leads in a new era of self-service in banking.[28] Automated Teller Machine is a computerized machine that offers

[27] Online available at en.wikipedia.org/wiki/Automated-teller-machine

[28] Online available at http://www.history.com/topics/inventions/automated-teller-machines, accessed on 14/06/2015 at 7:43 a.m.

customers the service of accessing their account for supplying cash and to carry out other financial & non-financial transactions without the need to actually visit their bank branch on placing of an encoded plastic card.[29]

ATMs generally accept ATM debit cards, credit cards and prepaid cards (that permit cash withdrawal) for various transactions. Bulk of ATM users use ATM to withdraw the cash, though, in addition to cash dispensing ATMs may have many other services/facilities allowed by the bank owning the ATM such as; Account information, Cash Deposit, Regular bills payment, Purchase of Re-load Vouchers for Mobiles, Mini Statement, Loan account enquiry etc. For transacting at an ATM, the customer has to insert /swipe the card in the ATM and enters Personal Identification Number (PIN) issued by the bank. Once PIN[30] is accepted by ATM, a customer can perform the transaction selected by them.[31] ATM allows the users to withdraw cash from the bank from any of its ATMs at any time so it is also known as 'Any Time Money' or 'Any Where Money'. ATM has become the most common and suitable way of delivery channel throughout entire country.[32]

2.1.3. ELECTRONIC CLEARING SERVICES

One of the electronic modes of funds transfer from one bank account to another is ECS[33]. It is used by institutions for making payments such as distribution of dividend

[29] RBI, DPSS.CO.PD. No. /02.10.002/2011-2012, February, 2012

[30] PIN is the numeric password which is separately handed over to the customer by the bank while issuing the card. Most banks require the customers to change the PIN on the first use.

[31] DPSS.PD.No. 2632/02.10.002/2010-2011 dated May 27, 2011

[32] Dr. Roshan Lal; Dr. Rajni Saluji, "*E-Banking: The Indian Scenario"*, Asia Pacific Journal of Marketing and Management Review, Vol. 1 issue 4, December 2012.

[33] Electronic Clearing Services.

interest, salary, and pension, among others. For payment of bills and other charges such as telephone, electricity, water or for making equated monthly instalments payments on loans as well as SIP investments can also be pay through ECS. ECS can be used for both credit and debit purposes. The main objective of Electronic Clearing services is to offer other method of payment transactions that would prevent the need for issuing as well as handling paper tools and thereby progress the payment efficiency and also provide better customer service by banks.[34]

The pace of banking businesses across the country was enhanced by the electronic payment systems such as Electronic Clearing Service, credit and debit or RTGS and National Electronic Fund Transfer.[35] These all services are one of the new electronic fund services. ECS is a non-paper based movement of funds which is encouraged by the RBI on a wide scale. ECS consists of- Electronic Credit Clearing Service & Electronic Debit Clearing Service.[36] National Electronic Fund Transaction (NEFT) is a deferred net settlement system and is an improvement over other modes in terms of security and processing efficiency. This facility is currently available at over 46,300 bank branches throughout the country.[37]

[34] Reserve Bank of India (Department of Payment and Settlement Systems Central Office, Mumbai-April-2011), https://rbidocs.rbi.org.in/rdocs/ECS/PDFs/ECR300411E.pdf, accessed on 14/06/015 at 10:15 a.m.

[35] Yazeed, Yazidu & Ibrahim, *"Automated Teller Machine (ATM) Operation Features and Usage in Ghana: Implications for Managerial Decisions",* Journal of Business Administration and Education, Vol. 5 No. 2, 2014, 137-157.

[36] Source: RBI, Report on Trend and Progress of banking in India, 2012.

[37] Dr. Roshan Lal; Dr. Rajni Saluji, *"E-Banking: The Indian Scenario",* Asia Pacific Journal of Marketing and Management Review, Vol. 1 issue 4, December 2012.

2.1.4. ELECTRONIC FUND TRANSFER

Electronic Fund Transfer (EFT) is the electronic transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, through computer-based systems and without the direct intervention of bank staff.

The term covers a number of different payment systems, for example:

- Using a payment card such as a credit or debit card, cardholder can initiated the transaction.
- The payer can initiate the direct deposit payment system.
- Direct debit payments for which a business debits the consumer's bank accounts for payment for goods or services.
- Wire transfer through an international banking network such as SWIFT.
- Electronic bill payment in online banking, which may be delivered by EFT or paper check.
- Transactions involving stored value of electronic money, possibly in a private currency.

Electronic Fund Transfer (EFT) is a system of transferring money from one bank account to another. One of the mainly used EFT programs is Direct Deposit. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments.[38]

[38] Electronic Funds Transfer (EFT) Definition, sounce available at http://searchwindowsserver.techtarget.com/definition/Electronic-Funds_Transfer-EFT

2.1.5. ACCOUNT OPENING REQUEST

In an internet banking system the customers are able to open a new account through online. In a traditional banking system customers have to go into the branch for the opening of new account but in today's banking system customers need not visit bank for any banking business. This system of banking is much easier than the traditional bank. Customer can apply for a new account only in branches where they already have accounts. Customer should have an INB-enabled account with transaction right in the branch. Funds that are deposited by the customers in an existing account are used to open the new account.

While opening a new account, customers just need to visit the internet banking site with their ID and choose the new account opening ling under requests tab then the customers can see every types of account, what they are willing to openSelect the account and account type they wish to open and submit the same. Then, they need to select the branch and enter the initial amount to open the account. Customers can select any of their accounts for debiting the initial amount. Then, submit the transaction. Their new account opening request will be processed by the branch.

2.1.6. ACCOUNT STATEMENT

The Internet Banking request can create an online. If the customers want to see their account detail for any type of accounts for any date can be seen via online. They are also able to download these details. For account enquiry customers need not need to visit branch, they can enquire account details from anywhere at any time. They can see various kinds of details through online such as, the transaction details, opening,

closing and accumulated balance in the account Customer can generate the online account statement for any date range or for any month and year.

2.1.7. TRANSACTION ENQUIRY

An online bank provides features to enquire status of online transactions. Customer can view and verify transaction details and the current status of transactions. The VISA transactions can also be viewed separately by login on to retail section of the Internet Banking site with their credentials and select the Status Enquiry link under the Enquiries tab. They will be displayed all online transactions they have performed. To view details of individual transactions, customer needs to click the Transaction Reference number link. They are displayed the debit and credit account details, transaction amount, narration and transaction status.

Based on RBI's Report[39] of Internet banking the levels of banking services offered through internet can be categorized into three class:

1. The banks' website which provides information on various products and services which is offered by banks to their customers is the basic level service. In this form of banking customers' enquiry were received and reply through e-mail[40].
2. In the next level of internet banking services allows customers to submit their orders, requests for different services, enquiry on their account balances etc. are done through simple transactional websites, but do not allow any fund-based business on their accounts.

[39] RBI Report on Internet Banking, 2011
[40] ibid

3. The third level of internet banking services are allow the customers to function on their accounts for transfer of funds, payment of different bills and to transact purchase and sale of securities, etc. are presented by the *fully transactional website.*

"In India, ICICI bank was the first bank to offer online banking way back in 1996 with the launch of infinity"[41]. After ICICI Bank, Citibank, IndusInd Bank, HDFC Bank and Times Bank (now part of HDFC Bank), were the early ones to introduce online banking in India. At present, majority of commercial banks are offering internet banking service in India.

Presently banks in India provided different kind of online banking services to their customers. The security of information may be one of the biggest concerns to the internet users. For internet banking users who most likely connect to the internet via dial-up modem, is faced with a smaller risk of someone breaking in their computers. Only organizations such as banks with dedicated internet connections face the risk of someone from the internet gaining unauthorized access to their computer network.[42] However, the I-banking system users still face the security risks with unauthorized access into their banking accounts. Hackers have many different ways that they can by to break into systems. The problem of the systems today is inherent within the setup of the communications and also within the computers itself. So for the protection of such kind of fraud, banks provide pre-login security & privacy features and post login security & privacy features to their customers.

[41] Available at http://shodhganga.inflibnet.ac.in/bitstream/10603/71745/7/07_chapter%201.pdf, accessed on 07/02/2017.

[42] Supra note 40.

2.2. PRE-LOGIN SECURITY AND PRIVACY FEATURES

Keeping the eye in cyber crime Indian banking system has introduced a Pre Login security and Privacy Features. To use the Internet Banking services, a customer has to login to his internet banking account with User Id and password. Bank issues 'User Id' and 'Password' to customer at the time of opening of account either as a part of 'Welcome Kit' or at special request of the customer. Pre-Login features are those features of online portals which a customer comes across at the time of login to his account. There are number of pre-login features of online banking portals. However, keeping in mind the scope of the study, only security and privacy related features have been compared[43].

It is easy for a customer to login to online banking portal from home page of main website itself. Furthermore, the risk of web spoofing[44] is less, if customers access online banking portal from home page of the bank.

The next security feature of online portals is compulsory entry of 'One Time Password', if a customer login to his/her internet banking account from different browsers the access to the site will be allowed only after entering OTP[45] i.e. one time password which will come on his/her mobile phone via SMS. This feature makes online portals more secure and prevents unauthorized access.

[43] Dr. Tejinderpal Singh, *"Security and Privacy Issues in E-Banking: An Empirical Study of Customers' Perception",* p. 95 online available at www.iibf.org.in accessed on 25th oct. 2016 at 7:45 p.m.

[44] Web page spoofing is an activity that hackers use to direct Web site visitors to a Web site that looks like the one they believe they are visiting.

[45] A one-time password (OTP) is a password that is valid for only one login session or transaction.

Another security feature is the virtual key of online banking portals. While using virtual key board[46], a customer has to enter authentication details such as user-id password by clicking the on-screen keyboard instead of hard keyboard. [47]Virtual key board secures the websites from key-loggers. All banks' online portals have the option of using virtual keyboard. However it is used as an optional in nature[48].

Recently, two more forms of virtual key board have been introduced to provide more security to login process. These forms are 'Scrambled Keyboard' with 'Shuffle' option and 'Hovering Keyboard'. 'Scrambled Keyboard' is an application which is both virtual and dynamic in nature when customer login.[49] In the more advance form, the position of characters on the keyboard changes every time, a character is inserted through the 'Virtual Keyboard' if 'Shuffle' option is on. On the other hand, 'Hovering Keyboard' is a new innovation, which helps customers to enter their banking password by just pointing mouse on the relevant character. This is also called as 'Mouse over'.

Multi-Factor Authentication (MFA) strengthens security at login time by using an additional form of 'authentication' beyond the standard username and password. The solution is designed to preserve the convenience and usability of online banking while providing additional security for customers. Banks permit up to five attempts for wrong entry of password. More attempts will result in blocking of password. Hence, there must be alert for the customers about leftover attempts which will warn them

[46] A virtual keyboard is a software component that allows a user to enter characters. A virtual keyboard can usually be operated with multiple input devices, which may include a touchscreen, an actual computer keyboard and a computer mouse.

[47] Source available at http://irjrr.com/irjrr/November2015/5.pdf

[48] Online available at www.paloaltonetworks.com accessed on 25th Oct. 2016 at 2:35 p.m.

[49] Ibid.

before entering wrong password. It avoids inconvenience to the customers because of password block. It is general practice that banks alert the user by putting security and privacy messages either on the login page or before the login page.

2.3. POST-LOGIN SECURITY AND PRIVACY FEATURES

Post-Login feature are those features which customers come across after login to their internet banking account. Some of the bank clearly instructs that, if user ID is not used for 360 days it will expire automatically. Such instructions prevent unauthorized use of user ID. Internet banking portals display the last login time and date on web page to alert the internet banking users. User may easily recall time and date of their last visit to the site. If they had not visited the site, it will alert them to take due action.

Online security experts always advise that one should change one's password frequently. However, it is general tendency among internet users that they hardly change their passwords. Same is the case with internet banking users. When any online transaction takes place through online banking, a SMS is sent to user's mobile phone to alert him about the transaction. All banks send mobile alert messages to their customer for online transactions. With this facility, online banking users may immediately notice, if any unauthorized transaction takes place.

There is always risk, if someone leaves online line banking portal unattended while logged in. In this case another person may use online banking portals in absence of genuine customer. Banks have introduced the facility of 'Idle Time log out' where user is automatically logged out after defined time.

There is another security feature of online banking portals i.e. Backspace', 'Fresh', 'Forward' logout where pressing of any of these buttons will result in automatically logout from the portal.

Presently banks in India provided different kind of online banking services to their customers. The security of information may be one of the biggest concerns to the internet users. For internet banking users who most likely connect to the internet via dial-up modem, is faced with a smaller risk of someone breaking in their computers. Only organizations such as banks with dedicated internet connections face the risk of someone from the internet gaining unauthorized access to their computer network.[50] However, the I-banking system users still face the security risks with unauthorized access into their banking accounts. Hackers have many different ways that they can by to break into systems. The problem of the systems today is inherent within the setup of the communications and also within the computers itself. So for the protection of such kind of fraud, banks provide pre-login security & privacy features and post login security & privacy features to their customers.

[50] Supra note 40.

CHAPTER III

3. A COMPARATIVE OVERVIEW OF INTERNET BANKING SERVICES IN VARIOUS COUNTRIES

Internet banking is a banking products and services offered by banking institutions on the Internet through access devices, including personal computers and other intelligent devices. Internet banking remains one of the economical and more efficient delivery channels. According to *Arunachalam* and *Sivasubramanian*, Internet banking is where a customer can access his or her bank account via the Internet using personal computer (PC) or mobile phone and web-browser[51].

Even though the years have same days, same months, same hours, from the beginning of the time in today's world people are so busy in their day to day activities they do not get ample time to complete their work online banking appears to be a boon for the people. Online banking was introduced in the early 80s; with this many people have benefited from these facilities. Now a day, people do not have to wait at the bank or at some shopping centre or boutique for long hours. Online banking gives a person facility to view account statements, make money transfers from one account to the other, and also to pay funds. The best thing about online banking is that it is fast and is available to a person in any part of the world, at any time he or she needs it.

It might be surprising to learn that online banking has actually been around since the early 1980s. However, when 'online banking" became popular in the late 1980s, it use to have a very different meaning than it does today. Originally, the phrase referred to

[51] Asiimwe Balamu, *"Electronic Banking and Financial Performance of Commercial Banks: A Case Study of Stanbic Bank, Mbarara Branch"*, Research Report submitted on May 2015. Online available at www.academia.edu

the use of a terminal, keyboard and television or computer monitor to access one's bank accounts using a landline telephone. Online banking started in New York in 1981 when four city's major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services.[52] At the time, customers didn't really take to the initiatives, so it failed to gain momentum until the next wave of innovation in the mid-1990s.[53] In this chapter I am going to study about the Internet Banking laws of some of the country with compare to Indian laws.

3.1. USA

When the term "online banking" gained popularity in the late 1980s, the phrase referred to the use of a terminal, keyboard and television or computer monitor to access one's bank account using a landline telephone was defined as online banking. Whereas in today's world the online banking or internet banking is defined to anything that, includes electronic payment system that allows customers of a financial institution to conduct financial transactions through the financial institution's website. Today, online banking services include mobile internet banking technology, such as person-to-person payment smart phone apps and text banking.[54]

3.1.1. ONLINE BANKING: THE EARLY YEARS

The early version of what was considered online banking began in 1981. Four of the major banks of U.S. i.e. Citibank, Chase Manhattan, Chemical Bank and

[52] History of online banking, source available at en.wikipedia.orgr/wiki/online-banking, accessed on 24/04/2016

[53] Supra note 46.

[54] Supra.

Manufacturers Hanover were the first place to test out the innovative way of doing business by providing home-banking services to their customers.[55] Throughout the history of online banking, the new method of banking was slowly adapted by the customers. In the beginning of 1980s, customers were not able to adjust to the new initiative, so the online banking system totally failed to gain momentum until the next wave of innovation in the mid-1990s.[56]

In the U. S., Stanford Federal Credit Union became the first financial institution in the U.S. to offer internet banking to all of its customers in October 1994.[57] After that, Presidential Bank of U. S. offers customers access to their accounts online. Internet banking systems began to hold up because many banks followed the Presidential Bank's lead. At the same time, Security First Network Bank became the first dedicated online bank in the land of United States. S.F.N.B opened its doors for business with an offer for national online banking, including no-fee checking and an ATM card.[58]

The evolution of internet banking made their continuity with the first truly successful internet-bank, The Net-Bank. The Net-Bank was founded in 1996 and closed in 2007. The Net-Bank was acquired by *BofI* Federal Bank in 2012.[59] USA Bank of Internet

[55] Supra.

[56] Shilpan D. Vyas, *"E-Banking and E-Commerce in India and USA",* source available at https://ai2-s2pdfs.s3.amazonaws.com/6644/b854bdc2c8705497ab183d8697c893c6a97a.pdf

[57] Richard Sylla, *"The US Banking System: Origin, Development and Regulation",* source available at https://www.gilderlehrman.org/history-by-era/hamiltoneconomics/essays/us-banking-system-origin development-and-regulation

[58] Bob Batchelor, *"The History of E-Banking",* online available at http://www.ehow.com/about5109945 history-ebanking.html, accessed on 24/04/2016

[59] Ibid.

was officially found as a part of incorporation of the *BofI* Holding, and on July 6, 1999, making it America's oldest internet bank.

The convenience nature of internet banking became more obvious to many customers than that of traditional banking due to their high interest rates than those of regular banks, greater access to accounts, and online banking transfers, etc. However, not all the people were convenienced with online banking. Still customers were hesitant at first to use this new banking method because they were unsure of how it worked and didn't trust the security features of online banking.

3.1.2. ONLINE BANKING IN THE 2000s

As the online banking made its way to 2000s it began to gain popularity in e-commerce too. When the big banks began to offer online products and services, internet banking gained legitimacy for consumers. By 2000, online banking had become main-stream for banking: An overwhelming 80 percent of banks in the U.S. along were offering internet banking services. In 2001, Bank of America made history as it became the first financial institution to gain more than 3 million online banking customers.[60]

In 2009, Ally Bank joined the ranks of internet-only banks. As the consumer preferred online banking more than traditional banking," *Diane Morais*, the integration

[60] Kenneth D. Jones and Tim Critchfield, *"consolidation in the U.S. Banking Industry: Is the "Long Strange Trip" About to End",* FDIC Banking Review, Vol. 17 No. 4, 2005, pp. 31-61.

executive of Ally Bank[61] launched an Ally Bank brand to provide customers with customer-centric approach.

The survey of 2010 on consumer billing and payment trends, Fiserv found that online banking and mobile payments were at a faster pace than the internet. Online banking has continued to evolve as it offers more innovations and conveniences to the customers. In USA Bank of Internet has introduced a new and technologically advanced products and services since its inception, including mobile internet banking apps for the mobile, My Deposit for check deposit by mobile or computer scan, Pop money for money transfer via text or email, and EMV-chip debit cards.[62]

Online banking today has been spread widely that the customers expect accounts to include free online banking. The effective decrease overhead costs offer more competitive rates and enjoy higher profit margins to the banks. "As an online bank, Ally doesn't have branches, it offers the customers great rates, 24/7 service, and innovative and competitive deposit products,"

[61] Ally Financial Inc. (NYSE: ALLY) is a leading digital financial services company and a top 25 U.S. financial holding company offering financial products for consumers, businesses, automotive dealers and corporate clients. Ally Bank, the company's direct banking subsidiary, offers an array of banking products and services.

Deposit products ("Bank Accounts" on Ally.com) are offered by Ally Bank, Member FDIC. In addition, mortgage products are offered by Ally Bank, **Equal Housing Lender**, NMLS ID 181005. The Ally CashBack Credit Card is issued by TD Bank, N.A. Credit and collateral are subject to approval and additional terms and conditions apply. Programs, rates and terms and conditions are subject to change at any time without notice.

[62] Karen, William and Daniel, *"Internet Banking: Developments and Prospects",* Economic and Policy Analysis Working Paper 2000-9, online available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.201.3399&rep=rep1&type=pdf

3.1.3. POSITION OF REGULATORY FRAMEWORK OF INTERNET BANKING IN USA

There is a medium of legislation and regulations within the US that specifically codifies the use of rights associated with the Internet and e-commerce in general, and the electronic banking and Internet banking activities. Federal and state laws, regulations, and court decisions, and self-regulation among industries groups provide the legal and operational support for Internet commerce and banking in the USA. The international model laws promoted by the United Nations Commission on International Trade Law (UNCITRAL) provided the guidance to the member nations on the necessity for revising existing legal structures to accommodate electronic transactions. Important laws for general application to commercial activity over the Internet within the US are as follows:

1. Uniform Commercial Code (UCC), the Uniform Electronic Transaction Act (UETA) provides the electronic documents and contracts that should not be disqualified as legal documents because of their electronic form, various state laws and regulations on digital signatures and national encryption standards and export regulations. State laws in various areas may vary, but the trend is towards creating legislation, which is technology neutral.[63]

2. The E-sign Act, is a new US law that came into effect on October 1, 2000, which validates contracts that are concluded by electronic signatures and equates them to those signed with ink on paper. Under this Act, electronic signatures using touch-tones (on a telephone), retinal scans and voice recognition are also acceptable ways to enter into agreements. The E-sign Act takes a technological neutral approach and does not

[63] The Uniform Electronic Transaction Act, 1999

promote the use of any particular technology to validate an electronic document. However this act does not address issues relating to which US state's laws would govern an online transaction and which state's code would have jurisdiction over a dispute.[64]

3. The Gramm - Leach – Bliley (GLB) Act has significantly eased the restrictions on the ability of banks to provide financial services. It has established new rules for the protection of consumer financial information. The Inter-agency Statement on Electronic Financial Services and Consumer Compliance (July 1998) addresses consumer protection laws and describe how they can be met in the context of electronic delivery. In addition, the Federal Reserve Board has issued a request for comment on revised proposals that would permit electronic delivery of federally mandated disclosures under the five consumer protection regulations of the FRB which are (Regulations B, DD, E, M &Z)[65]. The Interpretive Ruling Office of the Comptroller of Currency (OCC) authorizes a national bank to perform, provide or deliver through electronic means and facilities. The concerns of the Federal Reserve are limited to ensuring that Internet banking and other electronic banking services are implemented with proper attention to security, the safety and soundness of the bank, and the protection of the bank customers. Currently, all banks, whether they are 'Internet based banks' or traditional banks must apply for a charter according to existing guidelines. The five federal agencies - Federal Deposit Insurance Corporation (FDIC), Federal Reserve System (FRS), Office of the Comptroller of Currency (OCC), Office of Thrift Supervision (OTS) and the National Credit Union Association

[64] The E-sign Act, 2000.

[65] Reserve Bank of India Report on Internet Banking dated 22 jun 2001, online available at http://www.rbi.org.in/scripts/PublicationReportDetails, accessed on 22nd may 2016.

(NCUA) supervise more than 20,000 institutions. Each state has a supervisory agency for the banks that is charter.[66] Most financial institutions in the US face no prerequisite conditions for an existing banking institution to begin electronic banking. For these banks, supervisors gather information on electronic banking through annual examination. Newly chartered Internet banks are subject to the standard chartering procedures. However, OTS has instituted a 30-day advance notification requirement for thrift institutions that plan to establish a transactional web site, and some State banking departments have instituted a similar requirement for transactional Internet banking web sites.

All the policy, licensing, legal requirements and consumer protection are generally similar for electronic banking and traditional banking activities. However, in response to the risks of electronic banking, federal banking agencies have issued supervisory guidelines and examination procedures for examiners who review and inspect electronic banking applications. Even though banks have been using specialize procedures in some areas of Internet banking activities, the existing information technology examination framework that addresses access controls, information security, business recovery and other risk areas generally continues to be applicable. In order to supervise the monitor the expansion of Internet banking, state chartered and national banks has been required since June 1999 to report their websites' 'Uniform Resource Locators' (URL) in the Quarterly Reports of Financial Condition that are submitted to supervisors. In addition, examiners review the potential risk associated with web-site information or activities, the potential impact of various Internet strategies on an institution's financial condition, and the need to monitor and manage

[66] Richard J. Sullivan, *"How has the Adoption of Internet Banking Affected Performance and Risk in Banks?",* Financial Industry Perspectives-2000.

foreign relationships. To check lab to test and validate the security of software and hardware used by banking organizations these risks, the OCC is on the verge to develop specific guidance for establishing 'Internet only' banks within the US. The Banking Industry Technology Secretariat recently has announced the formation of a security. If a bank is relying on a third party provider, it is accepted that it should be able to understand the provided information security programme to effectively evaluate the security system's ability to protect bank and customer data. Federal banking agencies conduct a operation i.e, "Examination Of Service Provides" where necessary following to the Bank Services Company Act, solely to support supervision of banking organizations.[67]

The Federal Financial Institutions Examination Council (FFIEC) introduced the Information Systems (IS) rating system that are utilized by central and state supervisors to consider uniformly financial and service giver threats initiated by information technology. And to recognized those organisations and service providers wants special supervisory attention. The FFIEC has recently renamed the system as Uniform Rating System for IT (URSIT), which has enhanced the audit function, and has been upgraded for the importance of risk management procedure.

Some characteristics of e-money products such as:

i. the relative lack of physical bulk,

ii. the potential anonymity and;

[67] Kenneth D. Jones and Tim Critchfield, *"consolidation in the U.S. Banking Industry: Is the "Long Strange Trip" About to End",* FDIC Banking Review, Vol. 17 No. 4, 2005, pp. 31-61.

iii. the possibility of effecting fast and remote transfer; has made them more susceptible than traditional systems to money laundering activities. The OCC guidelines lay down an effective policy known as 'know your customer'. Federal financial institutions, such as Society for Worldwide Interbank Financial Telecommunications (SWIFT) and Clearing House Interbank Payment System (CHIPS) have issued and regulated statements encouraging participants to include information on originators and beneficiaries.

'The Right to Privacy' in 1890 was published in the *Harvard Law Review* by Professors Samuel D Warren and Louis D Brandeis, the legal protection of privacy in civil society has been recognised in the United States common law. Moreover, as the US system has focused on technological innovation from the conception of The Right to Privacy by Warren and Brandeis, and for protecting privacy in the commercial realm. The Harvard professors astutely noted that 'recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual […] the right "to be let alone"'. In 1974, US Congress enacted the federal Privacy Act for regulating government databases, and after that it is found that 'the Constitution of United States provided that the right to privacy is a personal and fundamental right'. It is generally acknowledged that the US Privacy Act represented the first official embodiment of the fair information principles and practices and it has been incorporated in many other data protection regimes including the European Union's 1995 Data Protection Directives.

Other than the Privacy act the other sector of recent legislative activity in Washington, Congress has not been able to act on privacy, consumer data security, data breach notification or cyber security legislation. With the Administration of President Obama,

he has called upon a Congress session to enact a 'Consumer Privacy Bill of Rights' and legislation to help protect cyber security for 'critical infrastructure', partisan gridlock, as well has viewed his concern about over-regulating the private sector, that has stalled action.[68]

Due to the ECHR directives, US had to enact the "Safe Harbour Principles (SHP)" however, the provisions of SHP has not been totally compliant of the EU Directives, it has been approved by the European Commission the Safe Harbour Principles of US in the year 2000. The main objectives of SHP are to protect information and its privacy, free flow of information and to promote e-commerce. The US views the private data as a commodity whereby if a person wants to barter his private data against discounts offered by a departmental store he is free to do that. If the discounts are worth more to a consumer rather than his privacy, he or she can sign up for the same which will allow retailers to tract his spending habits.

With regard to data collection, SHP has the following features:

1. Notice: Notice need to be given to the consumer explaining about the need to collect data, and it should state the purpose of data collection, for what it will be used and how will it be used, and who will have access to it and how the data will be kept secured.
2. Choice: The data consumer should have choice to opt out of the collection and forward / transfer the data to third parties.
3. Access: The consumer should be provided access to data and to validate the personal information and to rectify it and to delete any erroneous information.

[68] Alan Charles Raul, *"The Privacy, Data Protection and Cyber Security Law Review",* published by *Law Business Research in November 2014, Edition-1.,p.270*

4. Third Party Transfer and Adherence: Every Third Party to whom data is sent should comply with the provisions of SHP.
5. Date Integrity: Data must be relevant and reliable for the purpose it was collected for.
6. Security: Reasonable protection and security measures should be provided for protection of data.
7. Enforcement: Every organisation that has personal data has to guarantee its adherence to SHP, examine and amicably settle consumer complaints and report violations of SHP.

3.2. U.K.[69]

Almost simultaneously with the United States, online banking arrived in the United Kingdom. In 1983 the first electronic banking service was introduced in the Nottingham Building Society, Britain through the joint venture with *Prestel*, i.e. a computerized information service owned by British Telecom[70].

The UK's first online/digital banking services known as *Homelink* were set up by Bank of Scotland for customers of the *Nottimghum* Building Society (NBS) in 1983. The system used by them was based on the UK's *Prestel* view-link system, such as the BBC Micro, or keyboard connected to the telephone system and television set, which allowed online viewing of statements, bank transfers and bill payments. If a consumer wants to make bank transfers and bill payments, a written instruction detailing of the intended recipient had to be sent to the NBS, who then set the details up on the Home-

[69] United Kingdom.

[70] Bob Batchelor, *"The History of E-Banking",* online available at http://www.ehow.com/about_5109945_history-ebanking.html accessed on 12/10/2016 at 2:34 p.m.

link system.[71] Most of the recipients were gas, electricity and telephone companies and accounts with other banks. Details of payments to be made were input into the NBS system by the account holder through *Prestel*. A cheque was then sent by NBS to the payee and hence an advice giving details of the payments was sent to the account holder.[72]

3.2.1. POSITION OF REGULATORY FRAMEWORK OF INTERNET BANKING IN UK

In UK, failure to undertake the procedure of identification of new customers properly can lead to the serious risks for the bank. Under the Data Protection Act, a bank faces an action for damages if it fails to — maintain adequate security precautions in respect to the data. Essentially, a legal duty is imposed particularly upon the banks to use reasonable care and skill in providing information to persons who access the bank's networks either on the internet or through an ATM card.[73]

The Computer Misuse Act of 1990 UK[74] states a similar objective as Data Protection Act. It is provided under "section (1) A, If person is guilty of an offence:

a. If he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; (b) the access he intends to secure, or to enable to be secured is unauthorized; and (c)

[71] Supra note 26.

[72] Francesca & Peter, *"Internet Banking in Europe: a comparative analysis",* Research Institute of Applied Economics- 2008.

[73] The Data Protection Act, 1998.

[74] This piece of legislation can be accessed at http://www.legislation.gov.uk/ukpga/1990/18/section/3.

he knows at the time when he causes the computer to perform the function that that is the case.[75]

b. The intent a person has to have to commit an offence under this section need not be directed at any particular program or data; a program or data of any particular kind; or a program or data held in any particular computer. Research Institute of Applied Economics 2008

c. A person guilty of an offence under this section shall be liable on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; (b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; (c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both".[76]

This position of the law was once given judicial interpretation where the views of the Judge were well applied to the Act. This was in the English case of *Barker v. Wilson*[77] it was stated that "The Bankers' Books Evidence Act was enacted with the practice of bankers in 1879 in mind. As now we understand the act, that it must have been construed in 1980 in relation to the practice of bankers. Therefore, construing the definition of "bankers books and the phrase on entry in a banker's book", it seems that both phrases are clearly apt to include any form of permanent record kept by the bank of transactions relating to the bank's business made by any of the methods w hich modern technology makes available."

[75] UK The Computer Misuse Act of 1990

[76] See also similar wording in the Computer Misuse Act of Singapore, retrived from http://unpan1.un.org/introduc/groups/ublic/documents/apcity/unpan002107, on 11th July 2016

[77] [1980] 2 ALL E.R. 80 at page 82

The case started a revolutionary move towards the English evidence practice, where for the first time the court recognized the changes brought by information and communication technologies (modern technologies) in proving bankers' books on data protection.

The United Kingdom has enacted the Data Protection Act, 1998 in agreement with the EU Directive. The Act has been elaborate and it defines important terms like "Data", "Data Subject", "Personal Data" as under:

"Data" means information which[78]—

1. Is being processed by means of equipment operating automatically in response to instructions given for that purpose,
2. is recorded with the intention that it should be processed by means of such equipment,
3. is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
4. does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

"data subject" means an individual who is the subject of personal data;

The Eight UK Principles for Data Protection are contained in Schedule - I[79] of the said Act. They are as follows:

1. There should be fair and legal processing of data.

[78] Data Protection Act, 1998.

[79] Supra.

2. Data Controllers should ensure that data is used only for lawful and specified purposes and should not carry out any processing which is incompatible with those purposes.
3. Data Controller should hold only personal data that is adequate and relevant and not excessive in relation to the purpose for which it is held.
4. All personal data are accurate and up to date.
5. Personal data shall not be kept for longer than necessary for the specified purpose or purposes.
6. Processing of personal data should be carried out in accordance with the rights of the data subjects under the Act.
7. Adequate, appropriate, technical and organisational measures should be taken against unauthorised or unlawful processing and accidental loss, destruction or damage to the personal data.
8. Data Controllers are obligated not to transfer data to countries that do not have adequate level of data protection. [The Eight Principle is in line with Article 25 of the EU Directive]

3.3. AUSTRALIA

In the late 80s and early 90s 'home banking' was rolled out, allowing customers to check their account balances from their home computer.[80] Internet banking in Australia is categorised in two forms; 1.web-based and 2.provision of proprietary software. Initial web-based products have focused on personal banking whereas the provision of proprietary software has been targeted at the business/corporate sector. Most Australian-owned banks and some foreign subsidiaries of bank have

[80] History of online internet banking in Australia, available at http://www.canstar.com.au/online-banking/history-of-internet-banking/, assessed on 21/10/2016 at 8:43 p.m.

transactional or interactive web-sites. Online banking services range from FI's websites providing information on financial products to enabling account management and financial transactions. Customer services offered online include account monitoring (electronic statement, real-time account management, bill payments, fund transfer, applying for products online) and financial transactions (securities trading, foreign currency transactions). Electronic Bill Presentment and payment (EBPP) is at an early stage. Features offered in proprietary software products (enabling business and corporation customers to connects to the financial institutions (via dial-up/ leased line/extranet) include account reporting, reconciliation, direct payments, payroll functionality and funds transfer between accounts held at their own or other banks. Apart from closed payment systems (involving a single payment-providers). Internet banking and e-commerce transactions in Australia are conducted using long-standing payment instruments and are cleared and settled through existing clearing and settlement system. Banks are involved with third party vendors or with outside providers for a range of products and services including e-banking. Generally, in Australia there are no 'virtual' banks and no license are issued to operate virtual bank in Australia[81].

The Electronic Transactions Act, 1999 provides certainty about the legal status of electronic transactions and allows Australians to use the internet to provide Commonwealth Departments and agencies with documents which have the same legal status as trade *foritional* paperwork. The Australian Securities and Investments Commission (ASIC) is the Australian regulator with responsibility for consumer aspect of banking, insurance and superannuation and as such, it is responsible for

[81] Supra note 73.

developing policy on consumer protection issues relating to the internet and e-commerce.[82]

3.4. INDIA

Internet banking is recently started in India. The rigorous use of IT in the banking sector started immediately after the recommendations of the Committee on Financial System *(Narasimham Committee,* 1991) were implemented in 1991. The *Narasimhan* Committee recommended that free entry of private sector and foreign banks. The private and foreign banks brought new technologies such as ATMs, credit cards and internet banking and rendered technology based world class quality services to their customers, which PSU banks, hitherto, were not even dreamed about. Indian banking depended upon the branch banking system for a century seems to have no place today. ICICI Bank was the first bank which lunched the internet banking system in the year 1996. After that Citibank and HDFC banks were provided internet banking service in 1999. To facilitate the advancement of internet banking in India, several measures have been taken by the Government of India as well as the Reserve Bank of India. The Government of India passed the Information Technology Act, 2000. This Act came to an effect from October 17, 2000. The main aim of IT Act, 2000 was to provide legal recognition to electronic transaction and other means of electronic commerce. The Reserve Bank is the banker's bank so that they administer and review the legal and other needs of internet banking on a continuous basis. RBI issued many guidelines for the advancement of internet banking on sound lines and internet banking related risks

[82] "*Vidyo Selected by Indusland Bank for First "Face-to-Face" Online Banking in India",* source available at http://www.vidyo.com/company/news-and-events/press-releases/vidyo-selected-indusind-bank-first-face-face-online-banking-india/, accessed on 13/10/20156 at 8:18 AM.

would not cause a danger to financial stability. A secure mode of transferring funds from one bank branch to another bank branch is a National Electronic Fund Transfer (NEFT), which is introduced in October 2005, is a nation-wide electronic payment system. An innovator in visual communications has been selected by Indus Ind Bank, one of the fastest growing new-generation private sector banks in India for Video Branch, a mobile and desktop-based banking service being deployed across the country. Video Branch, launched on June 2, 2014, has accumulated a user rating of 4.8 on scale of 5 on the Google Play Store.[83]

In Indian context has right to privacy as Fundamental rights which is provided under Article 21 of our Constitution and online privacy protection is being provided in Information Technology Act[84], 2008 as well in other scattered statues like SEBI's regulation and RBI's Guidelines to protect online privacy in electronic banking system.

Under Information Technology Act, 2008 there are some provisions like Section 43, *that provide for Penalty and Compensation for damage to computer, computer system,* Section 43-A provide to inter alia that Where a body corporate, possessing, dealing or handlinganysensitive personal data or information in a computer resource which it ow ns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five corer rupees, to the person so affected generally it

[83] Vidyo Selected by Indusland Bank for First "Face-to-Face" Online Banking in India, online available at http://www.vidyo.com/company/news-and-events/press-releases/vidyo-selected-indusind-bank-first-face-face-online-banking-india/, accessed on 13/10/2016 at 8:18 AM.

[84] Information Technology Act, 2008

provide compensation for failure to protect data, Section 44[85] provide penalty for failure to furnish information, return, Section 66-E[86] provide punishment for violation of privacy.

Internet banking is a popular and convenient method of doing online banking transactions but there is no dedicated Internet banking laws in India. However, Reserve Bank of India (RBI) has been consistently making efforts to bring more make internet banking transactions more and more secure. During the year 2010, Reserve Bank of India set up a Working Group under the Chairmanship of S.R Mittal to address the Regulatory and Supervisory concerns in i-banking focusing on i) Legal

[85] Section 44: Penalty for failure to furnish information return, etc. If any person who is required under this Act or any rules or regulations made thereunder to— (a) furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure; (b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues; (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

[86] [Section 66E] Punishment for violation of privacy. (Inserted Vide ITA 2008): Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both Explanation - For the purposes of this section-- (a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons; (b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means; (c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast; (d) “publishes” means reproduction in the printed or electronic form and making it available for public; (e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that-- (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

and regulatory issues, (ii) Security and technology issues and (iii) Supervisory and operational issues[87].

To facilitate the advancement of internet banking or to maintain the privacy and confidentiality of the customer information or to protect the customer from cyber crime, US government passed a different Act such as the Uniform Electronic Transaction Act, The E-Sign Act and The Gramm Leach Bliley Act. And in UK there is only one Act of Legislation such as The Data Protection Act which has contained all the provisions relating to cyber space. And in Australia there is no any appropriate legislation for internet banking. But in India, all the banks were regulated by the Reserve bank of India Act, 1934 and to provide legal recognition to electronic transaction and other means of electronic commerce, the government of India enacted the Information Technology Act, 2000. Hence, there was no separate law to regulate internet banking in India.

[87] Vide RBI Circular, DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01, June 14, 2001.

CHAPTER IV

4. ISSUES OF INTERNET BANKING

After analysing the data like Government notification relating to internet banking, Research Papers, Articles, Books, authentic website (official or private), different Act of Legislation, RBI guidelines on internet Banking etc., researchers came to know that the broadly use of information technology by banks has put them into the pressure to offer confidentiality and integrity of information. However, information systems and the internet banking businesses have been facing verity of security threats from a wide variety of sources including computer-assisted fraud, espionage, sabotage, vandalism etc[88]. There are various types of damage which have become more common in the internet banking environment, such as the computer viruses, computer hacking, phishing, denial of service attack, card skimming etc. The ever-growing reliance of banks on the information systems has made them more susceptible to such security threats. This has made it vital for every bank to put adequate security controls measures to certify data accessibility to all the authorized users and data inaccessibility to all the unauthorized users as well as maintenance of data integrity.[89] In the light of above, the present chapter presents the overview of legal, security and privacy issues in i-banking services.

[88] RBI Reports on Information Systems Security Guidelines for the Banking and Financial Sector (Part 1 and 2) dated: 11 Mar 2002, online available at https://www.rbi.gov.in accessed on 22nd oct. 2016.

[89] Dr. Tejinderpal Singh, *"Security and Privacy Issues in E-Banking: An Empirical Study of Customers' Perception",* A Micro Research Project Report (2012-2013).

4.1. PROBLEM RELATING TO ONLINE OPENING OF ACCOUNT:

The first problem involving to I-banking is the issue relating to online opening of account. The banks providing Internet banking service, at present are willing to accept the request for opening of accounts only on online submission even. On the other hand the accounts are opened only after proper physical introduction and verification of the customers. This is for the purpose of proper identification of the customer as well as to avoid *benami* accounts and money laundering activities that might be undertaken by the customer. RBI issues guidelines to all banks for opening an account through Internet, bank must opened an account only after proper introduction and physical confirmations of the character of the customer but private banks are not following the guidelines properly in order to raise their business they are opening an account without the proper verification of customers identity. This amount to non-compliance of the RBI directive "Know Your Customer" and makes the whole system vulnerable to attacks.

4.2. PROBLEM OF AUTHENTICATION AS WELL AS BANKS IN INDIA LAG IN SECURITY OF CARD TRANSACTIONS:

Second major problems faced by banks involved in internet banking is the issue relating to authentication as well as banks in India lag in security of card transactions. The present legal regime does not set out the restrictions as to the extent to which a person can be bound in respect of an electronic instruction purported to have been issued by him. Generally, authentication is achieved by security procedure such as methods and device like the relationship numbers, telephone-PIN numbers, and personal identification numbers (PIN), code numbers, passwords, account numbers and encryptions are developed to set up authenticity of an instruction. Security issues are important because these fraudsters can become serious to an individual in his life.

One can be a victim of a cyber crime in several ways. Against the background of well known global cases of card breaches, the banks in India have not been adopted that the basic measures for ensuring card security. Banks still follow storing and printing authorization information like non masking of card numbers, and CVV numbers and expiry dates which is a highly risky practice. Banks are permitted to create card records in plain text. All of such practices which is followed by banks are "non-conformant to globally accepted practices for card security. Some of these card and currency frauds are described below:

- **Skimming**

Skimming is known as "the act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card"[90]. The devices which are used by the fraudsters to capture cardholder information from the magnetic stripe on the back of an ATM card are known as Card skimming. These sophisticated devices are installed inside or over top of an ATM's initially installed card reader and which are smaller than a deck of cards. When the customer inserts his ATM card into the ATM machine, the skimmer captures the card details before it passes into the ATMs card reader to start the transaction and after removed from the ATM, a skimmer permits the download of personal information.[91]

Sometimes fraudsters can theft customer's card information through other fraudulent devices such as by converting cameras or keypad overlays which capture the consumer's PIN as which has been entered on the keypad during a transaction.

[90] Available at http://www.webopedia.com/TERM/C/card_skimming.html, accessed on 07/02/2017

[91] Skimming Detection & deterrence for Convenience Store ATM Owners, source available at http://www.securetransportassociation.org/files/resources/ATM_Skimming_Detection_and_Deterrence_Guide.pdf accessed on 27th Oct. 2016.

- **Card Trapping/Fishing**

Card trapping and fishing attempt is that where the fraudsters can theft consumers' card itself rather than information on it. Card trapping and fishing attack is arising only after card is inserted into the card reader. The main objective behind card trapping or fishing attack is to steal the card of a customers' and after that use it at a later time to make fraudulent withdrawal from the customers' account. Card trapping is carried out by inserting a tool over or inside the card reader slot to capture the consumer's card.[92]

- **Logical/data Attacks**

One of the most harmful attacks in term of quantity of consumer data can be the logical attack. This attacks target on ATM's software, operating system and communications system.[93] Fraudsters of logical attack included vandals who create viruses with an aim to exploit an ATM machine and hackers will install malware viruses to infringe the privacy, integrity or legitimacy of transaction related data.

- **Physical Attacks**

Any type of physical attack which causes harms the components of the ATM in an attempt to get cash is known as physical attacks on an ATM. While a physical attack can target the entire ATM as well as specific components of the ATM are often

[92] M. Mahbub Hasan, "Biometrics Technology can protect Cyber Crime on E- Banking System in Bangladesh", published on 25th july 2016.

[93] Tejinderpal Singh & Manpreet Kaur (2012), *"Internet Banking: Content Analysis of Selected Indian Public and Privte Sector Banks'* Online Portals, Vol. 17, No. 1, pp. 1-7, source available at http://www.iibf.org.in/documents/reseach-report/Tejinder_Final%20.pdf

targeted. There are many specific component which may be targeted are Safe, Top Hat, broadcaster and saver.

Most of the banks have put in place security provisions such as SMS alerts, a virtual keyboard and a separate transaction password for online banking, but this is not sufficient. To make card transaction secure, RBI has issued a guidelines to all the banks should introduce secure features for card transaction such as one- time-password, risk- based authentication and an identity grid etc., but most of the banks have still not introduced that features for secure card transaction. Some may steal user ID and password by trying over several attempts or by an intelligent guess. Banks are constantly being exposed to sophisticated, planned and financially motivated threats and customers are being targeted through different kind of cyber crime such as phishing, *vishing* and *smishing* attacks. Furthermore attack may involve installing of 'spyware' and 'Trojans' software which discover that what is going on in the PC, the fraudster can collect information from the PC and web links through web links and e-mail attachments. A hacker could also get to the ID and password through unauthorized access. With all this money being transferred online, online fraudsters try to intercept financial transactions and turn them to their benefit. From a legal viewpoint, the safety method needs to be provided by law as an alternative for signature. In India, "under section 3 (2) of the Information Technology Act, 2000 provides that any subscriber by affixing his digital signature may authenticate an electronic record. However the Act only recognizes one particular technology as a means of authenticating the electronic records (viz, the asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record). This might lead to the doubt of whether the law would recognize the existing methods used by the banks as a valid method of authenticating the

transactions".[94] However not all kinds of Electronic Signatures are reliable and secure. It is for the reason that the Section 3A of the IT Act defines it to mean an electronic authentication technique considered to be reliable which is specified under the second schedule. These both are the provisions of IT Act but the technical protection and legal protection are not in synchronizations.

The Information Technology Act 2008 has made most of the cyber crimes and cyber offences "bailable". India has made its cyberspace a "free zone" and "safe haven" for cyber criminals and cyber offenders. He says that now even after committing hacking in India a person would be entitled to "bail" as a matter of right. There is nothing that prevents such cyber criminals from committing cyber crimes in India in the absence of a deterrent law. This has resulted in an increased spate of cyber crimes including hacking of the e-mail IDs of the Internet banking users and stealing of their money.

4.3. LIABILITY OF BANKS IN BILATERAL AGREEMENT ETC. -

The definition of consumer and provisions for rights and liability of the customers has been provided under Consumer Protection Act, 1986 thus banking customers are also comes under this Act, therefore the provision of the Act are also applicable to banking services as well.[95] The rights and liabilities of both the banks as well as customers are determined by the bilateral agreement between banks and customer. Sometimes the agreement contains the provisions which are contrary to the consumer's interest. In such a situation whether any agreement between bank and customer defining customer's rights and liabilities which are adverse to consumers than what is enjoyed

[94] IT Act, 2000.

[95] Source available at https://www.ukessays.com/essays/information-technology/regulatory-and-supervisory-issuesinformation-technology-essay.php

by them in the traditional banking scenario will be legally tenable? Also in case of unauthorized hacking how the liability in such a situation will be determined. Further in case of denial of service also. Although the Information technology Act contains the provision of penalty for denial of access to a computer system(s-43) and hacking (s-66), but when it comes to the determine the liability of banks the Act gives no clue.

India has also become one of the most common surveillance societies of the World. Confidential information is already vulnerable and with the proposed Indian plans of installing key loggers by law enforcement officers at cyber cafes, the same would exclude the use of cyber cafes for these purposes. Praveen Dalal said that, cyber cafés are not a good place to transact confidential matters yet with a poor Internet penetration in India this may still happen.

With a weak cyber law, lack of cyber security awareness and increasing e-surveillance initiatives in India, Internet banking disputes are bound to increase in India. The government is least bothered about these issues and ultimately the account holders would have to bear the financial losses.

4.4. PROBLEM RELATING TO PRIVACY AND CONFIDENTIALITY OF CUSTOMER ACCOUNT AND INADEQUACY OF DATA PROTECTION LAW

It is a duty of banks to maintain privacy and confidentiality of the customer's account, but in internet banking, banks obligations to maintain privacy and confidentiality is very difficult task. Despite all reasonable precautions, banks may be exposed to improved risk of liability to customers on account of breach of secrecy due to loss/

misplacement/ theft of customers' ID/PIN, denial of services[96] etc., because of hacking or other technological failures. The obligation of banks to maintain secrecy of customers account was dates back to 1924 where in a case popularly known as *Tournier* case[97], in this case it was held that customers financial information and the nature and details of his account should not disclose by banks to anybody, since it may affect his reputation, credit worthiness and business. Now with the advent of new technology, banks obligation to maintain secrecy and confidentiality of customer account is very difficult task because hackers can operate others account, but bankers are not in a position to trace them. They come to know only when the customer informs them of some irregularity in their transaction. The banks are lacking instituting adequate risk control measures to manage such risk. Internal management systems of banks are also not fully gear for the digital age. And adequate risk control measures are not apposite in India. It is impossible for banks to retain information solely within their own computer networks, let alone a single jurisdiction of data is sufficiently high. Banks are deficient in providing adequate legal and technical protection.

An individual's right to privacy has evolved out of Article 21[98] of the Constitution and other constitutional provisions protecting fundamental rights. Article 21 of the Constitution provides that no person shall be deprived of life or personal liberty except according to the procedure established by law. The Supreme Court of India has held in

[96] Denial of service attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

[97] *Tournier v. National Provincial & Union Bank of England*, (1924), K.B., 461.

[98] Protection of Life and personal liberty- no person shall be deprived of his life or personal liberty except according to procedure established by law.

a number of cases that the right to privacy is implicit in the right to life and personal liberty guaranteed to Indian citizens. However, constitutional rights can normally be claimed only against the State or State-owned enterprises and not against private individuals or establishments.

The Information Technology Act, 2000 ("IT Act") penalizes "cyber contraventions" (section 43(a) to (h)) and "cyber offences" (sections 65-74). The former category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. The latter category covers "serious" offences like tampering with computer source code, hacking with an intent to cause damage, and breach of confidentiality and privacy, all of which attract criminal prosecution. The IT Act also prescribes penalties for hacking, which is tampering with a computer's source code and any breach of confidentiality and privacy obligations by a person having powers under the IT Act.

Confidentiality obligations are limited to officers or persons having powers under the Act and do not extend to private persons. Further, the officer is not liable to compensate the person damaged by the disclosure. Moreover, most of the penalties are in the range of Rs.200,000 to Rs.500,000, which are very insignificant amounts when compared to the gains that a person may make from the crime.

In India, data protection issues are crucial as there is no separate law for data protection, though The Information Technology Act, 2000, in Section 72 has provided for penalty for breach of privacy and confidentiality. Further, Section 79 of the Act has also provided for exclusion of liability of a network service provider for data travelling through their network subject to certain conditions. Therefore, the liability of banks for breach of privacy and confidentiality when data is travelling through network is

ambiguous. The significance of data protection and privacy has been underscored in the IT Act, but many banks are still lacking in understanding of this issue. And also lack of adequate security and data protection measures which can make customers vulnerable to attacks from fraudsters and could result in hacking or misuse of their bank and credit card accounts.

Information Technology Act was passed in the year 2000, based on UNCITRAL model law on E-commerce but there was no single provision for data protection. But in 2008, Indian Parliament Amended the IT Act and incorporated few small provisions for protection of computer data by service providers, but these provisions are not adequate to protect the customers from the cyber frauds. Hence, there is a need to pass a separate law containing various provisions for data protection as well as internet banking frauds liabilities as UK having.

4.5. CYBER SECURITY OF BANKS IN INDIA NEEDS STRENGTHENING:

Indian cyber security has been ignored for many years by the previous governments making Indian computer systems and critical infrastructures vulnerable to sophisticated cyber attacks. One of the critical infrastructures is banking sector of India that has miserable cyber security infrastructure. The cyber security trends and developments in India have proved this point very well.

India has no dedicated cyber security laws and this is creating numerous troubles for various stakeholders. The banking sector of India is also neglecting cyber security in the absence of stem and effective cyber security regulatory norms in India. Cyber security compliances require adherence to certain well established legal principles. The moment a cyber security breach occurs, many legal issues and compliance

requirements are automatically invoked. For instance, in a typical cyber attack, it becomes imperative to ascertain and find the originator of such attack. The requirements to engage in first instance analysis, e-discovery and cyber forensic also arise due to such cyber attack. The reporting requirement to the compliance and regulatory authorities also arise.

However, none of this applies to Indian companies and individuals that are facing cyber attacks no matter howsoever sophisticated and damaging such cyber attack are in India companies and individuals are not reporting cyber security breaches and attacks to the government and its agencies.

The Indian government has in past declared that cyber security breaches disclosure norms of India would be formulated very soon. However, bill now no action has been taken in this regard and companies and individuals are still not reporting cyber security breached to Indian government and its agencies.

For instance, cyber crimes and cyber attacks against banks of India is a very common phenomenon in India. However, banks of India are not only lax while maintaining cyber security but they are also not disclosing such cyber crimes and cyber attacks due to fear of adverse publicity and regulatory penalties. This is creating more problems for the bank customers in general and banking cyber security in India in particular.

The Information Technology Act, 2000 (IT Act,2000) is the sole cyber law of India. However, it is not capable of forcing the companies and individuals to disclose cyber security breaches and cyber crimes. Nevertheless, the rules under IT Act, 2000 prescribe cyber law due diligence, internet intermediary, reasonable cyber security

practices etc. They indirectly cover some aspects of cyber security discloser norms. But they are not sufficient to meet the demand of present time.

Some basic level guidelines and recommendation have been issued by RBI such as internet banking guidelines, guidelines for secure electronic payment transactions etc., but they are far from satisfactory and being effective. RBI has also mandated establishment of Steering Committees on Information Security by Banks in India and appointment of Chief Information Officers (CIOs) for all banks in India. However, banks in India have failed to comply with the directions of RBI so far and even RBI has allowed them to take liberty. In effect, this means that there is neither a legal framework nor any compulsion to ensure cyber security of banks in India. Naturally, the online banking system in India is not at all cyber secure and banks in India are not following cyber security due diligence and cyber law due diligence at all.

Lastly In order for internet banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of internet banking can be very prosperous. The future of internet banking will be a system where users are able to interact with their banks “worry-free” and banks are operated under one common standard.

CHAPTER V

5. LEGAL FRAMEWORK OF INTERNET BANKING IN INDIA

India is also a member country of WTO. The basic aims of WTO are Liberalization, Globalization and Privatization. So that, in India trade and commerce has been liberalized. After liberalization of trade and commerce the financial sector has also undergone major changes. With the arrival of internet banking, India is facing unprecedented competition from the World at large. To compete with the world financial sector bank should update their technology as soon as possible. Without updating the technology in financial sector, international trade would be a distant dream. The deregulation of the banking industry coupled with the emergence of new technologies has enabled new competitors to enter the financial services market quickly and efficiently[99]. Internet banking is also regulated and applicable by those provisions of law which are applicable to traditional banking activity. The problem does not overcome by this law, and therefore there is a need for introduction of more strict rules and laws specifically to meet the problems of internet banking.

Branch Banking is regulated by set of enactment like the Banking Regulation Act, 1948, the Reserve Bank of India Act, 1949 and the Foreign Exchange Management Act, 1999. Apart from these, banking businesses were also influenced by several legislations governing trade and commerce, i.e., Indian Contract Act, 1872, the Negotiable Instruments Act, 1881, Indian Evidence Act, 1872, Bankers Books Evidence Act, 1891, etc.[100] Internet banking is an expansion of the branch banking,

[99] Dr. Suresh V. Nadagoudar & M. P. Chandrika, *"Law Relating to E-Banking in India- An Outreach Challenge",*

[100] Tannan, M. L. (2003), "*Banking Law and Practice in India"*, (20th Ed.), (New Delhi: India Law House, p.157

hence, various provision of law, which are related to branch banking activities, are also applicable to internet banking. However, use of electronic medium in general and internet in particular in banking transactions, has put to question the legality of certain types of transactions in the context of existing statute. The validity of an electronic message/document authentication, validity of contract entered into electronically, non-repudiation etc. is important legal questions having banking on electronic commerce and internet banking. The vulnerability of data/information passing through internet has also raised the issue of ability of banks to comply with legal requirement practices like secrecy of customers account, privacy, consumer protection etc.. There is also the question of adequacy of law to deal with situations which are technology driven like denial of services/data corruption because of technological failure, infrastructure failure, hacking, etc. Cross border transactions carried through internet pose the issues of jurisdiction and conflicts of laws of different nations. Therefore, the Reserve Bank of India has issued various internet banking guidelines for the protection of cyber crime such as; Internet Banking in India- Guidelines, Guidelines on electronic payments security transactions.

The security of information may be one of the biggest concerns to the internet users. For internet banking users who most likely connect to the internet via dial-up modem, is faced with a smaller risk of someone breaking in their computers. Only organizations such as banks with dedicated internet connections face the risk of someone from the internet gaining unauthorized access to their computer network.[101] However, the I-banking system users still face the security risks with unauthorized access into their banking accounts. Hackers have many different ways that they can by

[101] Ibid.

to break into systems. The problem of the systems today is inherent within the setup of the communications and also within the computers itself.

Security in internet banking companies both the computer and communication security. The main aim of computer security is to preserve computing resources against unauthorized use and abuse and to protect from accidental and deliberate damage, disclosure and modification. The communication security aims to protect data during the transmission in computer network and distributed system.[102] When people use the internet they expect confidentiality and data integrity. The volume of data being exchanged on the internet increases, so as the network security is become more and more crucial. Internet banking which required security-based system, there are various risks and internet fraud that can affect the customer's view of the service quality provided by the banks.

The most critical issue of internet banking security is to secure valuable information that susceptible to unauthorized access by attackers. Availability of confidential information which is secured by a user name and pin name or password, makes it vulnerable to such threats. Majority of banks have implementing latest network security software to make their sites secured.[103] Hence, the banks must constantly increase security.

This division between integration of trade and finance over the globe through e-commerce and divergence of national laws is perceived as a major obstacle for i-

[102] Marinela Vrîncianu and Liana Anica Popa, "*Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests", "Protection of Consumers' Rights and interests",* Volume-XII, Issue-28, June 2010, pp., 388-403.

[103] Kani, R. Melba, "*Security Issues in Online Banking Services*", "Indian Journal of Applied Research", Volume: 4 Issue: 3, March 2014, p.1

banking and has set in motion the process of harmonization and standardization of laws relating to money, banking and financial services. The General Assembly of United Nations has take a major initiative in e-commerce is the United Nations Commission on International Trade Law (UNICITRAl)'s Model law, and also has been recommended to the member nations for consideration while revising/adopting their laws of electronic trade.

Government of India has passed the Information Technology Act, 2000, in order to provide legal recognition for transactions carried out by means of electronic commerce and also known as electronic data interchange and other means of electronic communication, The Act, which has also drawn upon the model law, came into force with effect from October 17, 2000. The Act has also amended certain provisions of the Indian Penal Code, the Indian Evidence Act, 1872, The Bankers Book of Evidence Act, 1891 and Reserve Bank of India Act, 1934 in order to facilitate ecommerce in India. Further, The Information Technology Act, 2000 was amended in 2008.

5.1. MODEL LAW IN INTERNET BANKING

The articles 6[104], 7[105], 8[106] and 9[107] of the UNCITRAL Model Law and Commonwealth Model Law provides for functional similarity thus where the law

[104] Article 6. Compliance with a requirement for a signature 1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement. 2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature. 3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if: (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (b) The signature creation data were, at the time of signing, under the

control of the signatory and of no other person; (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable. 4. Paragraph 3 does not limit the ability of any person: (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or (b) To adduce evidence of the non-reliability of an electronic signature. 5. The provisions of this article do not apply to the following: [...]

[105] Article 7. Satisfaction of article 6 1. [Any person, organ or authority, whether public or private, specified by the enacting State as competent] may determine which electronic signatures satisfy the provisions of article 6 of this Law. 2. Any determination made under paragraph 1 shall be consistent with recognized international standards. 3. Nothing in this article affects the operation of the rules of private international law

[106] Article 8. Conduct of the signatory 1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall: (a) Exercise reasonable care to avoid unauthorized use of its signature creation data; (b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) The signatory knows that the signature creation data have been compromised; or (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised; (c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate. 2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

[107] Article 9. Conduct of the certification service provider 1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: (a) Act in accordance with representations made by it with respect to its policies and practices; (b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate; (c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate: (i) The identity of the certification service provider; (ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued; (iii) That signature creation data were valid at or before the time when the certificate was issued; (d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise: (i)

requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as the reliable as was appropriate for purpose for the data massage was generated or communicated, in light all of the above which circumstance, including any relevant agreement. It is believed that these Model Laws will assist states in reforming and enhancing their legislations that are on paper method and come up with uniform laws that allow the use of alternatives to paper based methods of transactions, communication and storage of information at national and international level.[108]

The leading piece of legislation at the International level is the UNCITRAL Model Law on Electronic Signatures. Article 6 (1) provide of the Model Law provides that ―where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.[109]

The method used to identify the signatory; (ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used; (iii) That the signature creation data are valid and have not been compromised; (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider; (v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law; (vi) Whether a timely revocation service is offered; (e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service; (f) Utilize trustworthy systems, procedures and human resources in performing its services. 2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

[108] Mambi, (2010), p.132

[109] UNCITRAL Model Law on Electronic Signatures

The Model Law defines electronic signatures as ―data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.[110] The Model Law defines certificate as a data message or other record confirming the link between a signatory and signature creation data[111] The data message is defined as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy."[112]

On reliability and security of electronic signatures, the Model Law provides that an electronic signature is considered to be reliable if first, the signature creation data are within the context in which they are used linked to the signatory and to no other person. Second, the signature creation data were, at the time of signing, under the control of the signatory and of no other person. Third, any alteration to the electronic signature, made after the time of signing, is detectable. Last, if any alteration made to that information after the time of signing is detectable. The purpose of these requirements is to assure integrity of the electronic records.

The analysis of these statutes demonstrates two important aspects. Firstly, an electronic signatures not to be denied admissibility as evidence in legal proceedings solely on the ground that it is in an electronic form. Secondly, those electronic signatures enjoy the same legal status as the paper- based signatures

[110] Ibid, Article 1.

[111] ibid

[112] ibid

5.2. BANKING SERVICES

Internet banking is defined as the use of Internet as a remote delivery channel of banking system services via the World Wide Web. All the banks of a whole world are increasingly offering online banking services: customers are checking their status and also transferring money from one account to another or investing in stock from their PCs at home and in the office. Customer can perform various tasks through internet banking, such as: viewing account balances, viewing recent transactions, downloading bank statements, for example in PDF format, ordering cheque books, download periodic account statement, viewing images of paid cheques, downloading application for I-banking, funds transfers between the customer's linked accounts, paying third parties, including bill payments and third party funds transfers, investment purchase or sale, loan applications and transactions, such as repayments of enrolments, credit card application, register utility billers and make bill payments etc.. With the rapid development of internet and computer technology has led to the growth of new forms of transaction, so modern banking increasingly relies on the internet and computer technology to operate their businesses and market interactions which led the growth of new forms of transactional crime especially internet related and the threats and security breaches are highly increase in recent years. So internet banking presents challenges to financial security and personal privacy when banks information is compromised by skilled criminal hackers by manipulating a financial institutions online information system. This causes huge financial losses to the banks and customers.[113] In the course of providing Internet banking services the banks in India are facing new challenges relating to online opening of account, authentication,

[113] Zakaria Karim, Mohammed Rezaul, Aliar Hossain, *"towards Secure Information System in Online Banking".*

secrecy of customers accounts, non-repudiation, liability standards and consumers protection, etc., each of which has been examined in the context of existing legal framework. Internet banking is an extension of the traditional banking; bank uses Internet as a medium for receiving instructions from the customers and also delivering banking services. So, conceptually, various provisions of law, which are applicable to traditional banking activities, are also applicable to Internet banking such as:

5.2.1. RESERVE BANK OF INDIA ACT, 1934

India's central banks are the Reserve Bank of India (RBI). Reserve Bank of India monitors, formulate and implements India's monetary policy. RBI was established in the year 1935, it was nationalized in the year 1949[114], which is owned fully by the Government of India. It was established in April 1935 with a share capital of Rs. 5 crores on the basis of the recommendations of the Hilton Young Commission. The Act, 1934 (II of 1934) provides the statutory basis of the functioning of the bank. In accordance with the provisions of the RBI, Act, 1934 the main functions as…. "to regulate the issue of Bank Notes and keeping of reserves with a view to securing monetary stability in India and generally to operate the currency and credit system of the country is to regulate the issue of Bank Notes and keeping of reserves with a view to securing monetary stability in India".[115]

Since the onset of the on-going liberalization and globalization of the economy, the role of the RBI as the regulator of the financial sector has grown and diversifies. All the banks in the country is regulated by the Reserve Bank of India and as a regulator, all the banks including commercial banks, also supervises co-operative banks, Non Banking Finance companies, Financial Institutions etc. thus the entire institutional

[114] M. L. Tannan, *"Tannan's Banking: Law & Practice in India"*, 21st Edition, 2005, p. 163.

[115] Reserve Bank of India Act, 1934.

function of providing finance comes under the regulatory oversight of the RBI. Therefore, all banks i.e. existing banks with traditional delivery channels or virtual banks/internet-only banks will functions their business under the regulatory framework of the Reserve Bank of India.

The Reserve Bank of India accepts and makes payment on behalf of Central Government. All the banking function of the Central Government such as carries out its exchange remittance, management of public debt and other banking function. *In India,* the Central Government entrusts its money, remittance, exchange and banking transactions with the RBI. It deals in repo or reserve repo. The banks listed in second schedule and non-schedule banks shall maintain a cash reserve ratio with the RBI with a view securing the monetary stability in the country. It provides loans and advances in foreign currency to scheduled banks and to other financial institution. It purchases, sells or discount any bill of exchange or promissory note or makes a loan or advances to schedule bank. The Reserve Bank of India is empowered to formulate all types of banking policy in the interest of the public. Therefore, RBI provides all types of policies relating to internet banking and which is to be followed by all the banks. Without obtaining the approval from RBI, no banks can commence banking business in India. The RBI grant license to commence banking business in India and they also have power to cancel a license granted to a banking company, if banks are not properly followed the RBI rules.

The Act will enable the RBI to issue new bank licenses to corporate houses and strengthen the RBI's hand with powers to supersede entire boards of recalcitrant banks that fail to comply with its directions. Before the amendment, the RBI only had powers to remove a director or officers of a banking company and not the full board. But with this amendment, the RBI will now have the power to supersede the entire

board, in public interest, and appoint an administrator to run the bank for a period not exceeding 12 months. The amendment will also increase the rates of existing monetary penalties that RBI can impose on a bank if it disobeys its rules and directives or gives false information.

As I explained above that internet banking is the extension of traditional banking, so all rules and regulations which is applied to the traditional banking is also applied in internet banking.

5.2.2. BANKING REGULATION ACT, 1949

Banking is defined in section 5(b) of the Banking Regulation Act as the acceptance of deposits of money from public for the purpose of lending or investment. Such deposits may be repayable on demand or otherwise and withdrawable by check, draft order, or otherwise. Thus, a bank must perform two essential functions; 1) Acceptance of public deposits, and 2) lending or investment of such deposits.

Accepting deposits from "public" implies that a banker accepts deposits from anyone who offers money for such purposes. However, a banker can refuse to open account for undesirable persons and further, the opening of account is subject to certain conditions like proper introduction and identification. The "Know Your Customer" guidelines issued by the Reserve Bank of India require Banks to follow certain customer identification procedures for opening of accounts for protecting the banks from frauds, etc., and also for monitoring transactions of a suspicious nature for the purpose of reporting to appropriate authorities for taking anti money laundering measures and combating financing of terrorism.

Under section 49-A[116] of the Banking Regulation Act, no organization other than a bank is authorized to accept deposits withdrawble by check.

In India, it is necessary to have a license from the Reserve Bank under section 22[117] of the banking regulation act for commencing or carrying on the business of banking.

[116] ***49-A. Restriction on acceptance of deposits withdrawable by cheque.—*** *No* person other than a banking company, the Reserve Bank, the State Bank of India or any other 3[banking institution, firm or other person notified by the Central Government in this behalf on the recommendation of the Reserve Bank] shall accept from the public deposits of money withdrawable by cheque

[117] ***22. Licensing of banking companies***.—*6*[(1) Save as hereinafter provided no company shall carry on banking business in India unless it holds a licence issued in that behalf by the Reserve Bank and any such licence may be issued subject to such conditions as the Reserve Bank may think fit to impose.] *(2)* Every banking company in existence on the commencement of this Act, before the expiry of six months from such commencement, and every other company before commencing banking business 7[in India], shall apply in writing to the Reserve Bank for a licence under this section: Provided that in the case of banking company in existence on the commencement of this Act, nothing in sub-section (1) shall be deemed to prohibit the company from carrying on banking business until it is granted licence in pursuance of 8[this section] or is by notice in writing informed by the Reserve Bank that a licence cannot be granted to it: Provided further that the Reserve Bank shall not give a notice as aforesaid to a banking company in existence on the commencement of this Act before the expiry of the three years referred to in sub-section (1) of Sec. 11 or of such further period as the Reserve Bank may under that sub-section think fit to allow. (3) Before granting g any licence under this section the Reserve Bank may require to be satisfied by an inspection of the books of the company or otherwise that 1*[* * *] the* following conditions are fulfilled, namely: *2 [(a)* that the company is or will be in position to pay its present or future depositors in full as their claims accrue; (b) that the affairs of the company are not being, or are not likely to be conducted in a manner detrimental to the interests of its present or future depositors;] *3[(c)* that the general character of the proposed management of the company will not be prejudicial to the public interest of its present or future depositors; (d) that the company has adequate capital structure and earning prospects; (e) that the public interest will be served by the grant of a licence to the company to carry on banking business in India; (f) that having regard to the banking facilities available in the proposed principal area of operations of the company, the potential scope for expansion of banks already in existence in the area and other relevant factors the grant of the licence would not be prejudicial to the operation and consolidation of the banking system consistent with monetary stability and economic growth; (g) any other condition, the fulfilment of which would, in the opinion of the Reserve Bank, be necessary to ensure that the carrying on of banking business in India by the

Every banking company has to use the word "bank" or part of its name (section 7 of the act) and no company other than a banking company can use the words "bank", "banker", "banking" or "banking company" as a part of the name or for the purpose of business.

5.2.3. INFORMATION TECHNOLOGY ACT

Government of India has enacted The Information Technology Act, 2000, in order *"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce".* The Act, which has also drawn upon the Model Law, came into force with effect from October 17, 2000. The IT Act, 2000 as amended, provides the

---

company will not be prejudicial to the public interest or the interests of the depositors.] 4[(3-A) Before granting any licence under this section to a company incorporated outside India, the Reserve Bank may require to be satisfied by an inspection of the books of the company or otherwise that the conditions specified in sub-section (3) are fulfilled and that the carrying on of banking business by such company in India will be in the public interest and that the Government or law of the country in which it is incorporated does not discriminate in any way against companies registered in India and that the company complies with all the provisions of this Act applicable to banking companies incorporated outside India.] [(4) The Reserve Bank may cancel a licence granted to a banking company under this section (i) if the company ceases to carry on banking business in India; or (ii) if the company at any time fails to comply with any of the condition imposed upon it under sub-section (1); or (iii) if at any time, any of the conditions referred to in sub-section (3) 1(and sub-section (3-A) is not fulfilled Provided that before cancelling a licence under Cl. *(ii)* or Cl. *(iii)* of s sub-section on the ground that the banking company has failed to comply with or has failed to fulfil any of the conditions referred to therein, the Reserve Bank unless it is of opinion that the delay will be prejudicial to the interests of the company`: depositors or the public, shall grant to the company on such terms as it may specify, an opportunity of taking the necessary steps for complying with or fulfilling such condition. (5) Any banking company aggrieved by the decision of the Reserve Bank cancelling a licence under this section may, within thirty days from the date on which such decision is communicated to it, appeal to the Central Government. (6) The decision of the Central Government where an appeal has been preferred to it under sub-section (5) or of the Reserve Bank where no such appeal has been preferred shall be final.]

banks to civil[118] as well as criminal[119] liability. The Information Technology Act, 2000 ("IT Act") penalizes "cyber contraventions" (section 43(a) to (h)) and "cyber offences" (sections 65-74). The former category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. The latter category covers "serious" offences like tampering with computer source code, hacking with an intent to cause damage, and breach of confidentiality and privacy, all of which attract criminal prosecution. The IT Act also prescribes penalties for hacking, which is tampering with a computer's source code and any breach of confidentiality and privacy obligations by a person having powers under the IT Act.

In India, "under section 3 (2) of the Information Technology Act, 2000 provides that any subscriber by affixing his digital signature may authenticate an electronic record. However the Act only recognizes one particular technology as a means of authenticating the electronic records (viz, the asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record). This might lead to the doubt of whether the law would recognize the existing methods used by the banks as a valid method of authenticating the transactions".[120] However not all kinds of Electronic Signatures are reliable and secure. It is for the reason that the Section 3A of the IT Act defines it to mean an electronic authentication technique considered to be reliable which is specified under the second schedule. These both are the provisions of IT Act but the technical protection and legal protection are not in synchronizations.

[118] Section 43-45 of ITAA, 2008.

[119] Sections 65-72 of ITAA, 2008.

[120] IT Act, 2000.

Under Information Technology Act, 2008 there are some provisions like Section 43[121], Section 43-A provide that "where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected". Section 44[122] provide penalty for failure to furnish information, return, Section 66-E[123] provide punishment for violation of privacy. Section 67[124], 67A[125], 67B[126] and some other section which directly and indirectly promote protection to data and privacy in electronic transactions.

[121] Penalty and Compensation for damage to computer, computer system

[122] Section 44: Penalty for failure to furnish information return, etc. If any person who is required under this Act or any rules or regulations made there under to— (a) furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure; (b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues; (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

[123] Section 66E: Punishment for violation of privacy, "Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both".

[124] Section 67 of ITAA, 2008,

[125] Section 67A of ITAA, 2008.

[126] Section 67B of ITAA, 2008 provides that, "*Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form*".

Phishing is a serious offence under Information technology Act .Section 66C of Information Technology Amendment Act, 2008, penalizes identity theft. The provision states that

"Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh."

In addition, Section 66D[127] of this Act provides that cheating by personation by using computer resource.

The Information Technology Act 2008 has made most of the cyber crimes and cyber offences "bailable". India has made its cyberspace a "free zone" and "safe haven" for cyber criminals and cyber offenders. He says that now even after committing hacking in India a person would be entitled to "bail" as a matter of right. There is nothing that prevents such cyber criminals from committing cyber crimes in India in the absence of a deterrent law. This has resulted in an increased spate of cyber crimes including hacking of the e-mail IDs of the Internet banking users and stealing of their money.

5.2.4. RBI GUIDELINES ON INTERNET BANKING

When people use the internet they expect confidentiality and data integrity. The volume of data being exchanged on the internet increases, so as the network security is become more and more crucial. Internet banking which required security-based system, there are various risks and internet fraud that can affect the customer's view of

[127] Section 66D of ITAA, 2008, provides that, "Punishment for cheating by personation by using computer resource".

the service quality provided by the banks. Therefore, Reserve Bank of India issues various guidelines or circulars to the Banks to provide secure internet banking services to their customers and banks have to follow these. Banks were advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. These 'Know Your Customer' guidelines have been revisited in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued. Banks have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated with the approval of their Board and put in place[128].

The Reserve Bank of India has issued New 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 customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank. Internet banking is a popular and convenient method of doing online banking transactions but there is no dedicated Internet banking laws in India. However, Reserve Bank of India (RBI) has been consistently making efforts to bring more make

[128] RBI Vide Circular DBOD. AML. BC. No. 11/14.01.001/2012-13

internet banking transactions more and more secure. During the year 2000, Reserve Bank of India set up a Working Group to examine different issues relating to i-banking and recommend technology, security, legal standards and operational standards keeping in view the international best practices.[129] And again in the year 2010, Reserve Bank of India set up a Working Group under the Chairmanship of S.R Mittal to address the Regulatory and Supervisory concerns in i-banking focusing on i) Legal and regulatory issues, (ii) Security and technology issues and (iii) Supervisory and operational issues. Major recommendations of the Group accepted by RBI have been listed as under.[130]

I. Technology and Security Standards:

a. Banks should designate a network and database administrator who will ensure that only the latest versions of the licensed software with latest patches are installed in the system, proper user groups with access privileges are created and users are assigned to appropriate groups as per their business roles, a proper system of back up of data and software is in place and is strictly adhered to, business continuity plan is in place and frequently tested and there is a robust system of keeping log of all network activity and analyzing the same. (Para 6.2.4)

b. Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems. (Para 6.3.10, 6.4.1)

[129] Vide RBI Circular, DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01, June 14, 2001.

[130] Vide RBI Circular, DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01, June 14, 2001.

c. Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies. (Para 6.4.2)

d. At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank‘s system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert. (Para 6.4.3)

e. All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server. (Para 6.4.4)

f. PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. However, as it is not yet commonly available, banks should use the following alternative system during the transition, until the PKI is put in place:

1. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the banks themselves using a Certificate Server.
2. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself. (Para 6.4.5)

a. It is also recommended that all unnecessary services on the application serve such as FTP (File Transfer Protocol), telnet should be disabled. The application server should be isolated from the e-mail server. (Para 6.4.6)

b. All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be reported and follow up action taken should be kept in mind while framing future policy. Banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the endusers on a continuous basis. (Para 6.4.7, 6.4.11, 6.4.12)

c. The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:

1. Attempting to guess passwords using password-cracking tools.
2. Search for back door traps in the programs.
3. Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.
4. Check if commonly known holes in the software, especially the browser and the e-mail software exist.
5. The penetration testing may also be carried out by engaging outside experts (often called _Ethical Hackers‘). (Para 6.4.8)

g. Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats. (Para 6.4.9)

h. Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank‘s security policy. Business

continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically. (Para 6.4.10)

i. All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form. (Para 6.4.13)

j. Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control. (Para 6.4.15)

II. Legal Issues

a. Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer. (Para 7.2.1)

b. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk. (Para 7.3.1)

c. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to

customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks. (Para 7.5.1-7.5.4)

d. In Internet banking scenario there is very little scope for the banks to act on stop-payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted. (Para 7.6.1)

e. The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks**.** (Para 7.11.1)

III. Regulatory and Supervisory Issues:

As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:

1. Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.

2. The products should be restricted to account holders only and should not be offered in other jurisdictions.
3. The services should only include local currency products.
4. The in-out' scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the _out-in' scenario where Indian residents are offered banking services by banks operating in cross-border jurisdictions are generally not permitted and this approach will apply to Internet banking also. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.
5. Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor. Given the regulatory approach, RBI advised banks to follow the following instructions:

a. All banks, who propose to offer transactional services on the Internet, should obtain prior approval from RBI. Bank's application for such permission should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners, third party service providers and systems and control procedures the bank proposes to adopt for managing risks. The bank should also submit a security policy covering recommendations made in this circular and a certificate from an independent auditor that the minimum requirements prescribed have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services / products offered by them. (Para 8.4.1, 8.4.2)

b. Banks will report to RBI every breach or failure of security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks. (Para 8.4.3)

c. The guidelines issued by RBI on _Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will equally apply to Internet banking. The RBI as supervisor will cover the entire risks associated with electronic banking as a part of its regular inspections of banks. (Para 8.4.4, 8.4.5)

d. Banks should develop outsourcing guidelines to manage risks arising out of third party service providers, such as, disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks' systems and misutilizing the same, etc., effectively. (Para 8.4.7)

e. With the increasing popularity of e-commerce, it has become necessary to set up Inter-bank Payment Gateways' for settlement of such transactions. The protocol for transactions between the customer, the bank and the portal and the framework for setting up of payment gateways as recommended by the Group should be adopted. (Para 8.4.7, 8.4.9.1 – 8.4.9.5)

f. Only institutions who are members of the cheque clearing system in the country will be permitted to participate in Inter-bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intra-bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway. (Para 8.4.7)

g. Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as far as possible, in real time. (Para 8.4.7)

h. Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL / 128 bit encryption must be used as minimum level of security. Reserve Bank may get the security of the entire infrastructure both at the payment gateway‘s end and the participating institutions’ end certified prior to making the facility available for customers use. (Para 8.4.7)

i. Bilateral contracts between the payee and payees bank, the participating banks and service provider and the banks themselves will form the legal basis for such transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law. (Para 8.4.7)

j. Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template. The banks should also provide their latest published financial results over the net. (Para 8.4.8)

k. Hyperlinks from banks’ websites often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business unrelated to banking. Hyperlinks from banks’ websites should be confined to only those portals with which they have a payment arrangement or sites of their subsidiaries or principals. Hyperlinks to banks’ websites from other portals are normally meant for passing on information relating to purchases made by banks’ customers in the portal. Banks must follow the minimum recommended security

precautions while dealing with request received from other websites, relating to customers' purchases. (Para 8.4.9)

As per revised guidelines[131] no prior approval of the Reserve Bank of India will be required for offering Internet Banking services.

Further, The Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (2010) was constituted, under the Chairmanship of *Shri G. Gopalakrishna*, Executive Director, RBI[132]. The Group examined various issues arising out of the use of Information Technology in banks and made its recommendations in nine broad areas. These areas were IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal aspects. Final guidelines[133] in the respective areas as mentioned above were issued to banks for implementation. Important guidelines with respect to security of internet banking are reproduced here.

Authentication practices for internet banking:

1. Authentication methodologies may involve three basic ―factors‖ of securities :

a. Something the user has (e.g., ATM card, smart card); and

b. Something the user is (e.g., biometric characteristic, such as a fingerprint).

2. Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The principal objectives of two-factor authentication are to protect the confidentiality of

[131] RBI/2005-06/71 DBOD No. Comp.BC.14/07.03.29/2005-06, July 2005.

[132] RBI/2010-11/494 DBS.CO.ITC.BC.No. 6/31.02.008/2010-11

[133] Supra note 90.

customer account data and transaction details as well as enhance confidence in internet banking by combating various cyber attack mechanisms like phishing, key-logging, spyware-malware and other internet based frauds targeted at banks and their customers.

Implementation of two-factor authentication and other security measures for internet banking:

In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for fund transfers through internet banking:

1. The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution‘s Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/ commercial); the customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information being communicated to both the bank and the volume of transactions involved.
2. Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems.
3. There is a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. However, it is observed that some banks still use weak user id/password based authentication for fund transfers using internet banking. For carrying out critical transactions like fund transfers, the banks, at the

least, need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like (a) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) or (b) OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token).

4. To enhance online processing security, confirmatory second channel procedures (like telephony, SMS, email etc) should be applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.
5. Based on mutual authentication protocols, customers could also authenticate the bank‘s web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the secure sockets layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. These are special SSL Certificates that work with high security Web browsers to clearly identify a Web site's organizational identity. It should, however, be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.
6. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.

7. Changes in mobile phone number may be done through request from a branch only.
8. Implementation of virtual keyboard.
9. A cooling period for beneficiary addition and SMS and E-mail alerts when new beneficiaries are added.
10. Customers should be advised to adopt various good security precautions and practices in protecting their personal computer and to avoid conducting financial transactions from public or internet café computers.
11. Risk based transaction monitoring or surveillance process needs to be considered as an adjunct.
12. An online session would need to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.
13. By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute a true multifactor authentication.
14. As an integral part of the two factor authentication architecture, banks should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. The banks should also consider, and if deemed appropriate, implement the following control and security measures to minimise exposure to man-in-the middle attacks:

a. **Specific OTPs for adding new payees**: Each new payee should be authorized by the customer based on an OTP from a second channel which also shows payee details or

the customer‘s handwritten signature from a manual procedure which is verified by the bank.

b. **Individual OTPs for value transactions (payments and fund transfers)**: Each value transaction or an approved list of value transactions above a certain rupee threshold determined by the customer should require a new OTP.

c. **OTP time window**: Challenge-based and time-based OTPs provide strong security because their period of validity is controlled entirely by the bank and does not depend user behaviour. It is recommended that the banks should not allow the OTP time window to exceed 100 seconds on either side of the server time since the smaller the time window, the lower the risk of OTP misuse.

d. **Payment and fund transfer security**: Digital signatures and key based message authentication codes (KMAC) for payment or fund transactions could be considered for the detection of unauthorized modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him, which means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.

e. **Second channel notification / confirmation**: The bank should notify the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.

f. **Session time-out:** An online session would be automatically terminated after a fixed period of time unless the customer is reauthenticated for the existing session to be

maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

g. **SSL server certificate warning**: Internet banking customers should be made aware of and shown how to react to SSL or EV-SSL certificate warning.

Securing Electronic Payment Transactions[134]

With the diffusion of internet banking, electronic modes of payment like RTGS, NEFT and IMPS have emerged as channels of funds transfer. Hence, it is important that such delivery channels would also be safe and secure. Recently, RBI has issued additional Security and Risk Mitigation measures for Electronic Payment Transactions[135] in this regard which are being reproduced as follows;

1. Customer induced options may be provided for fixing a cap on the value / mode of transactions/beneficiaries. In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon.

2. Limit on the number of beneficiaries that may be added in a day per account could be considered.

3. A system of alert may be introduced when a beneficiary is added.

4. Banks may put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.

5. Introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered.

[134] RBI/ 2012 -13/424 , DPSS (CO) PD No.1462 / 02.14.003 / 2012-13 February 28, 2013.

[135] Supra note 92.

6. The banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions.
7. Capturing of Internet Protocol (IP) address as an additional validation check should be considered.
8. Sub-membership of banks to the centralised payment systems has made it possible for the customers of such sub-members to reap the benefits of the same. Banks accepting sub-members should ensure that the security measures put in place by the sub members are on par with the standards followed by them so as to ensure the safety and mitigate the reputation risk.
9. Banks may explore the feasibility of implementing new technologies like adaptive authentication, etc. for fraud detection.
10. The above security measures under B (i) to (ix) are expected to be put in place by banks by June 30, 2013.

The Government of India as well as the Reserve Bank of India has been taken the several initiatives to facilitate the development of internet banking in India. The Government of India enacted the IT Act, 2000 with effect from October 17, 2000 and further this Act has been amended in 2008, which provide legal recognition to electronic transactions and other means of electronic commerce. The RBI is monitoring and reviewing the legal and other requirements of internet banking on a continuous basis to ensure that internet banking related challenges would not pose threats to financial stability. RBI has issue many guidelines regarding the security issue on internet banking. The last few years have witnessed an explosion of Information Technology (IT) based initiatives which have brought about a sea change in the banking sector of the country. The Reserve Bank has been at the forefront of IT initiatives with broad directions outlined by its IT Vision Documents. With the

security and privacy issues resolved, the future of internet banking can be very prosperous. The future of internet banking will be a system where users are able to interact with their banks “worry-free” and banks are operated under one common standard.

CHAPTER VI

6. CONTRIBUTION OF JUDICIARY IN INTERNET BANKING

In the last decade internet banking has taken a leap. The country has witnessed a wide range of change in the old traditional banking system prevalent in the country. The banking transaction has transformed from a paper base institution and long line of waiting in line over the bank counters to a faster and easier mode of electronic transactions such as ATM, Credit/Debit Cards, Online payments and transactions of cash. This transformation in the banking sector with the introduction of e-banking has come as a boon in the country. The customers of the banks have been given various facilities of easy transaction of their money through e-bankings, ATM machines, Credit/Debit cards, online payments, etc.

Although Internet banking is a boon in the country, but due to large ratio of literacy rate and lack of knowledge regarding the through and flow and twist and turns in the operation of internet banking many of the innocent peoples are easily swayed away by many such peoples who take to their advantage of these people innocence. These people lurk amidst us and with their cunningness deprive the hard earned money of the innocent and the ignorant ones. Such frauds are reported daily in alarming proportion and these fraudsters are reported to have been working in gangs.

This *malafide* practice of fraud and cheat has been a very troubling menace in the country and the Government has passed various legislations to deal with these hurdles in the progressive run of e-banking. Many efforts are put forth to educate the people about e-banking and alert them about the various types of frauds that may be played upon them.

The judiciary is one of the vital organ that plays the crucial role in the strict and stringent follow up of these legislations. And in the past years many cases involved with such problems of fraudulent transactions through A.T.Ms, dishonest practice of the banks and many more concerns of e-banking have been brought before the Courts of Law. The adjudicators being the ones trusted with meeting the proper ends of justice, through its various Courts and Tribunals has seen to it that the proper justice is carried out as per law. These various Courts and Tribunals while in functioning of meeting the proper ends of justice, while adducing the facts and circumstances of each case, and with proper appreciation of evidence put forth, applied their pristine judicial minds and have guided the proper and wide range of interpretation of these various legislations.

The matters of disputes and complaints of fraud during transactions through e-banking, ATMs and disputes regarding the services and security measures of the banks are brought before the courts and most of them being concerned with the Consumer Protection Act are brought before the Consumer Forums.

Amongst the cases that are brought before the Tribunals, maximum number cases are the ones of ATM frauds.

The e-banking is easy to operate and if one is not cautious enough he can also be easily cheated. The frauds done through e-banking lead to the importance of not sharing ones personal identification numbers and other account details with other persons. The operation of one's ATM card and disclosure of PIN number in the presence of other individual results in most of the frauds done through ATMs.

Complainant not titled to any relief under the grounds of having disclosed his PIN no:

The State Consumer Dispute Redressal Commission, West Bengal in Branch manager, S.B.I vs Sri Kanan Behari Sena[136] has specifically dealt upon the very issue of not sharing or disclosing ones PIN no with other people. The Facts of the case are as such:-

This Appeal is directed against the judgement and order passed by Learned District Forum, Purba Medinipur in case no. CC 27 of 2012 against the complaint with certain directions upon the OP Bank.

The Complainant/Respondent here is an account holder with ATM card facility with the OP Bank. On 24/10/11 at 6.08 a.m. he went to the ATM counter at Mecheda and after entering into the counter he noticed that there were two unknown persons standing inside the counter and they were talking to themselves. The Complainant operated the machine to withdraw money, but the result was 'SORRY UNABLE TO PROCESS'. The Complainant thought that there might have been some technical problems or link failure and then left the ATM counter. On the next date, that is, on 25/10/11 at 6.05 a.m. he went to the ATM counter situated by the side of the OP Bank and wanted to withdraw Rs. 10,000/-. After receiving the transaction slip the Complainant noticed that the balance amount was less by Rs. 50,000/-. On the same day after opening of the Bank the Complainant contacted the Manager who upon enquiry told that on the previous day the said amount was transferred to the SBI, ADB Branch, Pandua and the holder of that account was Pintu Karmakar. The Complainant

[136] Branch manager, S.B.I vs Sri Kanan Behari Sena on 27 November 2014.

believed that Pintu Karmakar with his associates by commiting fraud transferred the said amount to his account. The Complainant lodge complaint with the local P.S. and informed the D.I.G. (Operation), C.I.D., Bhabani Bhaban, Kolkata on 27/10/11. The bank did not take any step for such fraudulent transfer of money from one account to another. Under the circumstances, the complaint was filed before the Learned Forum.

After hearing the Submissions of both the parties and appreciation of the facts laid before the Hon'ble Tribunal the Commission rightly stated "We have heard the submission made by both side. Admittedly, on 24/10/11 the Complainant went to the ATM counter and found that two strangers were already standing inside the counter. From the petition of complaint it would appear that in presence of such strangers the Complainant operated the macine and having noticed 'SORRY UNABLE TO PROCESS' and left the ATM counter. It is the specific case of the Complainant that the said two strangers practised fraud and thus transferred the amount to the account of one Pintu Karmakar at Pandua. The Complainant has disclosed in the petition of complaint that he had suspected Pintu Karmakar as having committed such fraud with his associates. It is the settled principle of law as enunciated in the decision of the Hon'ble National Commission reported in 2011 (2) CPR 26 (NC) [State Bank India vs. K. K. Bhalla] that in view of the elaborate procedure evolved by Bank it is not possible for money to be withdrawn by unauthorized person from ATM without ATM card and knowledge of PIN. CCTV footage under the circumstances of the case will not come in the aid of the Complainant's case, in as much as, the Complainant operated the machine in presence of strangers. Moreover the Complainant lodged complaint with the Kolaghat P.S. on 26/10/11. Under such circumstances, we are of the considered view that there was no deficiency on the part of the Bank and the

Learned District Forum was not justified in allowing the complaint. The Complainant is not entitled to get any relief."

The banking sectors having introduced the facilities of e-banking and ATMs most of the transaction are done through ATMs. ATM cards have been introduced by the Banks upon their customers and provided with secret 4 digit PIN codes for its safe and secured usage. The Banks have the responsibility to ensure that the ATM card and its secret 4 digit PIN number safely reaches the customers and also the duty of the banks to communicate the importance of not sharing ones secret PIN numbers with others. Apart from this the bank is also entrusted not to make errors in dealing with the hard earned deposits of its customers. The bank in maintaining all the records of the transactions and ensuring no erroneous mistakes happens, fails to take proper caution and attention and errs in its services can lead to wrongful loss to the customers. And in case of fraudulent transaction due to the deficiency in taking proper measures on the part of the bank, the bank shall be liable to pay compensations.

Bank liable for deficiency in its services-

In **Punjab National Bank vs Sh. Harish Joshi, The State Consumer Redressal Commission, Uttarakhand, Dehradun**[137], the Learned Commission has held that the Bank is liable for Redressal for the losses to its customers resulted by the defect in its services.

The facts of the case, in brief, are that the complainant Sh. Harish Joshi has a Saving Bank Account No. 4954000100000133 with the Punjab National Bank, Champawat.

[137] Punjab National Bank vs Sh. Harish Joshi, The State Consumer Redressal Commission, Uttarakhand, Dehradun, First Appeal No. 101/ 2010.

The said account was opened on 19.02.2009 and the complainant had deposited sum of Rs. 12,400/- in the said account on 04.06.2009. The complainant also holds an ATM card No. 5126520038024241 issued by the opposite party-bank. The complainant has alleged that someone has withdrawn sum of Rs. 11,373.15/- from his account fraudulently between 06.06.2009 to 12.06.2009, while he had never used his ATM card during the said period. This fact came to his knowledge on 28.06.2009, when he withdraw Rs.500/- from ATM and the machine showed a balance amount of Rs. 26.85/- in his account. He got his passbook updated on 01.07.2009 and the passbook entries showed that the said amount of Rs. 11,373.15/- was withdrawn against various shopping transactions made at various places out of Champawat. The Complainant lodged a complaint with the Branch Manager of the bank. After a week, when he approached the bank again, he was told that his complaint was forwarded to the Head Office. The complainant has stated in his consumer complaint that he is a government servant and he was present in his office in Champawat on the dates when the ATM card had been used for shopping purposes. When the bank neither gave an explanation for the alleged withdrawal of money from complainant's account, nor credited the said amount in his account, the complainant filed a consumer complaint vide order impugned dated 09.04.2010 in the above terms. Aggrieved by the said order, the bank has filed this appeal.

The appellant's main contention is that it is a case of cyber fraud and it had advised the complainant to lodge an FIR with the Cyber Crime Cell. According to the appellant, the ATM card cannot be used unless and until the correct Pin/ Code of user/ cardholder is known to someone and, therefore, the complainant had shared the Pin/ Code with his colleagues and relations. Only an investigation by the Cyber Crime Cell can bring out the fact as to how and who had withdrawn the money. But the

complainant avoided such an investigation by not lodging the FIR as advised to him, probably with an apprehension that someone close to him may get implicated in the said fraud. Thus, the case being a case of cyber fraud, the consumer complaint was not maintainable before the District Forum. Further, as is evident, the appellant has not made any deficiency in service. In support of the contention, the learned counsel for the appellant pressed into service a decision dated 15.04.2010 of this Commission rendered in First Appeal No. 141 of 2009; **Dr. Prem Sagar Gupta Vs. Manager, State Bank of India**[138]**.**

We considered the submission made by the learned council for the appellant and also the facts of the case. The last column of the chart is for "Terminal Location" and it indicates that two of the transactions were made in "San Francisco" on 09.06.2009 and 10.06.2009. The time of the said transactions is not given. Eight transactions have been made at Mumbai on 06.06.2009, 09.06.2009, 10.06.2009, 12.06.2009, 12.06.2009, 12.06.2009, 12.06.2009 and 12.06.2009. Two transactions have been made at Gurgoan on 12.06.2009 and 12.06.2009. If the ATM card was used fraudulently at these places for shopping, then the ATM card must be a Visa Debit Card. Such an ATM card can be used for the withdrawal of money from ATM machine using the Pin/ Code (or password) as well as for shopping purposes. But while making a purchase, it is not necessary to tell the password to the seller. What is reqired is to produce the ATM card. We fail to understand as to how an ATM card can used on 09.06.2009 and 10.06.2009 in San Francisco and on the same dates, the card was used in Mumbai. Similarly, we fail to understand as to how the said card can be used on 12.06.2009 in Mumbai and also in Gurgoan. This shows that the appellant has

[138] Dr. Prem Sagar Gupta Vs. Manager, State Bank of India, First Appeal No. 141 of 2009.

not probed into the matter seriously and has not given any explanation. This certainly amounts to deficiency in services.

When the complainant brought the matter to bank's notice, it was the duty of the bank to probe into the matter and to find out as to how the money was withdrawn and who had withdrawn it. It is not the case of withdrawing money from an ATM machine, but it is the case of using ATM Visa Debit card for shopping. It would not be just to presume that the complainant had shared the password of his ATM card with his colleagues and relations because the password has nothing to do with the shopping transactions. If the details of transactions, as furnished by the appellant, are apparently disbelieved, there is no sense of lodging an FIR. Therefore, without making a deep probe into the matter, the appellant has simply stated that the complainant had shared the password of his ATM card with others and, thus, the person who knew the password had committed the fraud. In our opinion, such as such an explanation is unwarranted. The amount withdrawn is not a big amount in lacs or crores, so as to presume that fake duplicate cards (we don't know whether it can be done or not) were used at different places because if someone commits a fraud, he would do so for big amounts in lacs or crores and not for such petty amounts. The decision dated 15.04.2010 of this commission, as stated above, can not help the appellant firstly because the said appeal was not maintainable and secondly the facts of the case were different from the facts of the instant case. That was a case of withdrawal of money from ATM by the cardholder's representative and not a case of the use of ATM card for shopping transactions.

Therefore, the appellant has certainly made a deficiency in service by acting so indifferently in dealing with the complainant's complaint. The chances of some

technical faults in the system cannot be ruled out and the appellant did not care to consider this possibility, particularly when the statement of transactions appeared apparently to be highly impracticable. Since the appellant has not given any explanation, we have every reason to believe that the details of the transactions shown by the system are due to some technical error in the bank's system. Therefore, the appellant-bank is morally liable to pay the said amount to the complainant along with interest as directed by the District Forum. However, since the error in statement of transactions has not been made intentionally by any employee of the bank but it appears to be a technical error, it would not be just to direct the bank to pay compensation @Rs. 100/- per day. Therefore, the order impugned is to be modified to this extent.

Appeal is partly allowed. Order impugned dated 09.04.2010 of the District Forum is Modified to the extent that the order regarding payment of compensation @Rs. 100/- per day, is set aside. Rest of the order of the District Forum is confirmed. No order as to costs.

The customers are always made cautious about not falling into the traps of phishing and swishing attacks and if the customers even after being warned about this share their personal account details to others the bank cannot be held liable for any compensations and the loss is upon the customer alone.

Banks not liable for the negligence of the customers-

State Consumer Dispute Redressal Commission, Chennai in Alpha And Omega Diagnostics (l)... Vs Icici Bank Ltd[139] has rightly cited that the unauthorized fund

[139] Alpha And Omega Diagnostics (l)... Vs Icici Bank Ltd, First Appeal No. 740/2011 on 24 March 2014.

transfer became possible only because of the negligence on the part of the complainant in divulging confidential data to third persons. And that the complainant is solely responsible for his losses.

The case of the complainant is that they were having a Current Account with the opposite party bank, and they never opted for online transaction; but on 21-08-2009, they came to know that a sum of Rs. 1,10,000/- had been transferred through online fund transfer from their account to an account in State Bank of India, **Mizzoram**. They registered a complaint with the opposite party bank at 10 am on 22-8-2009, but they did not take immediate action to block the money from the State Bank of **Mizzoram**, and due to their negligence and deficiency in service, the money was withdrawn at the other end. Hence the complaint.

According to the opposite party, in spite of repeated warning given to its customers that they should not give information like password, pin number and account details related to internet banking to any other person, the complainant due to negligence divulged those information's to a fraudster who contacted the complainant by phishing Email. The averment of the complainant that the complainant never opted for any online transaction is totally false in view of the fact that they availed online transaction and carried out 6 online transaction on 27-3-2009, and 4 online transactions on 30-3-2009. The complainant received a spam mail and they were unaware that it was a phishing mail and had negligently responded to that mail which caused the loss to the complainant, and the opposite party is in no way responsible for the fund transfer. There is no deficiency in service on their part.

The District Forum considered the rival contentions and dismissed the complaint holding that the unauthorized online transfer was possible only because of the

negligence on the part of the complainant in divulging confidential data and that there is no deficiency in service on the part of the opposite party.

It is pertinent to note that the appellant/ complainant has made an averment in the complaint that they never opted for online transaction; whereas it is substantiated by the opposite party bank that the complainant availed online online fund transfer, by producing the account statement of the complainant with regard to online transaction that took place for 4 times on 30-3-2009 which is not dispute by the complainant, and as a matter of fact the complainant availed the online transaction facilities with the opposite party bank and carried out 6 online transactions on 27-3-2009, and 4 online transactions on 30-3-2009, and in the course of the online transactions, they parted with the information about their user name, password, and credit details paving the way to 3rd party to intrude into his account and transfer the amount unauthorisedly. Thus, we find that the unauthorized fund transfer became possible only because of the negligence on the part of the complainant in divulging confidential data to third persons. We therefore find that the complainant is responsible for this unauthorized online transfer from their account and the opposite party is in no way responsible or liable for it.

The District Forum has rightly held that there is no deficiency in service on the part of the opposite party and has rightly dismissed the complaint. There is no infirmity in the order of the District Forum and we agree with the finding and the decision of the District Forum dismissing the complaint.

In the result, the appeal is dismissed confirming the order of the District Forum dismissing the complaint. No order as to costs in the appeal.

The banks are required to maintain their standards of services and uphold the protection of its customer's accounts details and other details and make sure its security measures are not neglected. In case if there seems to be any fraud the same has to be communicated to the customers immediately and preventive measures are to be taken up immediately so as to ensure that no further loss is incurred by its customers.

At the instance of a criminal case being filed regarding the fraudulent transaction of any of its account, the banks are required to co-operate with the investigating agencies, even if the bank is the one receiving deposits resulting from fraud or false play of the other bank.

In **M/s. Raatronics, Shri. Ashish Goradia (Proprietor of 1),Mr. Sharad S. Goradia V/s. Central Bank of India & others**[140]. It has been held as follows:

Brief Facts of the Case as are as follows:

Complainants had opened an overdraft account no XXXXXX8475 on 16th April 2009 with Respondent No 1. Its customer identification no is XXXXXX5337. While submitting KYC Document complainant had given contact number as XXXXXX2461 and XXXXXX0992. Complainant No 3 was authorized signatory for the said account.

On 3rd May 2013 the available credit balance in the said account was Rs. 5,99,178.98/- plus unused OD fund of amount Rs. 10,80,000 by pledging. Also fixed deposit receipts of Rs. 12,00,000 was there in the said account.

[140] M/s. Raatronics, Shri. Ashish Goradia (Proprietor of 1),Mr. Sharad S. Goradia V/s. Central Bank of India & others, Complaint No. 35 of 2013 dated 21st October 2013

On 6th May 2013 at 2.00 pm Respondent No 1 informed to the complainant that a cheque issued for Rs 4,000 is going to be dishonored due to insufficient fund.

Upon viewing the accounts details on same day, complainant found that fund amounting Rs. 16,75,000 was transferred vide five fraudulent transactions.

Amount was transferred to two different accounts held with Respondent No 1 & 6. These fraudulent transactions were conducted on 4th May, 2013.

On 7th May 2013 when complainant visited Respondent No 1, they further learnt that the funds were further transferred from Respondent No 1 to various account held with Respondent 2 & 3.

Complainants state that they did not receive any SMS alert on their registered mobile for new beneficiary addition and for any fraudulent fund transfer. Complainants claim that there has been no change or disruption in the service of mobile and was working when the fraudulent transaction took place.

Complainant learned that their registered mobile number was changed in Respondent No 1 record without any written instructions/mandate from them.

Complainant intimated about fraudulent transaction to Respondent No 1 on 6th May 2013 and requested to block the fund and minimize the loss, but the Respondent No 1 acted very slowly which resulted in heavy loss to complainant.

Complainant lodged complaint with *Bandra Kuria* Police Station on 6th May 2013 and FIR under Section 419, 420 of IPC 1860 and Section 66C and 66D of IT Act 2000 was registered on 7th May 2013.

Interim order was issued on 29th November 2013 to release the frozen amount available with Respondent No 2, 3 and also to other banks

Complainant could recover Rupees 2,52,000 from Respondent No 2 (Rupees 40,000) & Respondent No 3 (Rupees 2,12,000).

Complainant is claiming damages Rupees 20,00,000 as compensation from the Respondent. Complainants also claimed for the return of fixed deposit receipts amounting to Rupees 12,00,000 which are kept with Respondent No 1 as a security against overdraft Account XXXXXX 8475. Complainant has paid application fee Rupees 43,000/- through demand draft.

In their written and oral arguments, Respondent No. 1 has made following points:

The complainant in his complaint is silent about IT infrastructure being used and security practices being followed for accessing net banking facility.

Complainant was also using Grid Card for Two Factor Authentication, details of which is only known to complainants. Grid card is unique and duplication of the same is not possible at the premise of the Respondent No 1. Grid card has twenty five values (Columns A to E and Row 1 to 5) out of which using permutation and combination any three values are used for authentication along with User ID & password. Additionally for any transfer transaction or updates in personal information of the customer profile at the Bank this Grid card authentication is performed. These three combinations are random and different for every transaction and do not repeat the combination.

Respondent submits that password required to access the net banking facility is only known to the complainant and the same is stored in hashed form on the banking servers which are secured and duly audited as per the requirements of the compliance and governing regulations.

Respondent submits that they immediately informed Complainant on 6th May 2013, when they observed that the funds were insufficient in account. Till that time even Complainants were not aware about those fraudulent transactions. At 16.00 hrs on 6th May 2013 complainant confirmed verbally that there were fraudulent transaction in their account. As soon as Respondent got information, they initiated action from their end and contacted the concern banks. Respondent even helped complainant to approach police on 6th May 2013 and to file FIR on 7th May 2013. This demonstrated the timey response by the Respondent. Respondent also provided prompt and timely information to the police station.

Regarding SMS alert about fraudulent transactions, Respondent submits that the details of complainants were not changed by visiting the branch in person but changed through online net banking.

Respondent Submits that there is no email account of the complainant associated with the Online Internet Banking of Respondent No 1 and hence question of email compromise or online Internet account compromise due to phishing or other known techniques does not arise.

Therefore respondent requests to dismiss the suit against Respondent 1 with costs, no payment of compensation and no return of Fixed deposit as they are lien and were pledged for increasing OD limit

In their written and oral arguments, Respondent No. 2 has made following points:

Anita, one of the beneficiary of fraudulent transaction had opened her account bearing no 6114081202, with this Respondent bank on 8th September 2011 after executing necessary KYC procedure. She submitted copy of PAN card as a identification proof.

Upon receipt of information about fraudulent transactions, this respondent immediately blocked the entire amount Rs. 41,488 and frozen the account.

Respondent submits that as per interim order of the Hon'ble Adjudicating officer, they transferred this entire amount on 3rd March 2014 to the complainants account.

Respondent also submitted an Affidavit of Apology for the delay caused in complying the interim order.

In their written and oral arguments, Respondent No. 3 has made following points:

Shankar Shah, one of the beneficiary of fraudulent transaction had opened his account with this Respondent bank on 5th March 2013. While opening an account he has submitted copy of PAN Card and MTNL Land line Bill. He also presented the cheque of Rs. 75,000/- of Bank of Baroda, *Saket* Branch, New Delhi. PAN Card and MTNL Landline bill submitted were checked and found to be genuine.

On 6th May 2013 two credits amounting to Rs. 2,36,780/- were received in his account though NEFT from *Vinod Kumar Sharma* holding and account with Respondent No 1. On receipt of this fund Shankar Shah withdrew Rs. 25,000/- through other bank ATM and on 7th May 2013 additional Rs. 25,000/- was withdrawn from other bank ATM using debit card issued to him.

In their written and oral arguments, Respondent No. 6 has made following points:

Funds from the fraudulent transactions were transferred to the account of Harish Kumar (Account No 1751607) and Abhay Pratap Singh (Account No 1740457). While opening bank account documents like copy of PAN Card, MTNL Bill and funding cheque were collected. The World Check Online Report was also obtained by Respondent before opening bank account.

Respondent bank has implemented a Transaction Surveillance Technology called "MANTAS" which has many scenario inbuilt into it to monitor the transactions undertaken including scenarios like monitoring new deposit accounts opened or large transactions undertaken.

The police has made investigations into the case and submitted the following report:

Complainant was using mobile number XXXXXX2461 which was registered with Respondent No 1 for all banking related transactions. Before the incidence of fraudulent transactions this mobile number was changed from XXXXXX2461 to 9999958457 by using computer system with IP address 116.203.229.151. This system is in the name of Anil, Delhi. This person is not traceable due to incomplete address.

Total five fraudulent transactions amounting Rupees 16,75,000 took place on 4th May 2013 and money was transferred to three accounts held with Respondent no 1 & 6.

Complainant was using the Grid Card issued by Respondent No 1 and password details of the same was available only with the Complainant.

Investigating officers visited at the addresses of beneficiaries of fraudulent transactions provided by various Respondent banks, but no one is traceable. All beneficiaries were staying on the rent and left the place earlier.

IP addresses (14.98.20.74; 14.96.210.65) of the computer systems which were used to carry out the fraudulent transactions is in name of *Sunita Mittal*, New Delhi. When investigating officer visited the address there was no one of this name and not even in the neighbourhood.

The learned Commission after critical examination & scrutiny of all the evidence place on record by all the parties and after covering all the corners of issues on disputes has observed as follows:

Banks have defaulted on multiple counts as enumerated earlier in my Analysis of this case. Their omissions fall within the ambit of Section 43A of the IT Act. Main negligence is of Respondent No 1 (Central Bank of India) and Respondent No 6 (Royal Bank of Scotland NV). Hence I order Respondent No. 1 and Respondent No 6 each to pay damages to the tune of Rupees 8,00,000 (Rupees Eight Lakhs Only) by way of compensation to the Complainant, within a month of this order, failing which compound interest of 12 percent compounded monthly will also be chargeable.

In **Dr. Vijay Gopal Kulkarni & Smt. Sushama Vijay Kulkarni Vs. SBI Card & Payment services Pvt. Ltd & Unknown Person**[141], this is a proceeding of a complaint filed by the Complainant for Adjudication under Section 46 of the Information Technology Act.

Brief Fact of the case are as such: The Complainant No. 1 is a Senior Citizen and a Medical Practitioner. The Complainant No. 1 received his first SBI Credit Card in the year 2008. After the expiry of this card in January 2013 he received another SBI Credit Card bearing no XXXX XXXX XXXX 6784. This card was used sparingly. Mobile No. XXXXXX 0168 was registered for the purpose of receiving alerts from the bank. The Complainant No 1 states that after January 2013, he never went abroad, he never used credit card at any other location other than his own house and his own personal computer. The complainant claims that his computer system is safe and secure with appropriate security precautions. The Complainants also hold saving bank account with SBI Bank. This account was used for making Credit card payments. The Complainants alleges that after the midnight of Sunday 30th June 2013, between 1:50 hrs to 2:20 hrs on 1St July 2013, within half an hour about six fraudulent transactions

[141] Dr. Vijay Gopal Kulkarni & Smt. Sushama Vijay Kulkarni Vs. SBI Card & Payment services Pvt. Ltd & Unknown Person[141], Complaint No. 11 of 2014 dated 28th February 2014

amounting Rs. 1,39,094.34 took place. The complainant came to know about these transactions when he received SMS on his mobile. Subsequently complainant disabled the credit card and lodged complaint with SBI. On 3rd July, 2013 Complainant made a police complaint with local police station. On 13th August 2013, complaint was also made with Cyber Police cell at Bandra Kuria Complex. Complainant states that as per Cardholder Agreement available on Respondent No. 1 website, "International Transactions" means the transactions entered into by the cardholder on his/her card outside of India, Nepal and Bhutan". Complainant claims that he has received SMS from the Respondent No 1 about this fraudulent transactions which indicates that he was very much within India. As per Respondent No 1 all these fraudulent transactions have occurred in Russia. Respondent claims that all transactions are valid as they have been performed in a Secure Electronic Commerce Environment and have been validated by complainant Card CVV and Date of Birth over the Internet. Complainant is claiming damages of Rupees 1,39,094 with interest and additional Rupees 60,000 as compensation from the Respondent. Complainant has paid application fee Rupees 7,000 through demand draft.

In their written arguments and oral arguments, Respondents 1 have made following points:

Complainant is disputing on the online transactions done at sprypay.ru-PETROZAVODSK amounting to Rs. 1,39,094.34 dated 1St July, 2013

All transactions were conducted in 3D secured mode. Card details have been validated to conduct these transactions.

These transactions were conducted in a Secure Electronic Commerce Environment and have been validated by complainant Card CVV number, Card expiry date and validated by VBV password (known to cardholder only), over the Internet.

There is no mobile number change observed in this case.

Respondent claims that, Complainant's Card was first enrolled on 215t January 2013 and there is no VbV (Verified by Visa) password change to conduct the disputed transactions. Forgot Your Password (FYP) was also not used to createnew VbV password.

Respondent claims that, card details were compromised over phishing mail or unsecured internet site.

The police has made investigations into the case and submitted the followingreport:

As per the letter received from the Respondent No 1, fraudulent transactions have occurred in Russia.

The fraudulent transactions were made from computer system having IP address 180.215.88.235. Cyber Police Station, Bandra Kurla Complex, Mumbai were requested to provide further details about the owner of this IP address. But no report is received from them.

In this case it has been held that the Bank has not given any meaningful, detailed report about the internal investigation into crime by their FIU (Fraud Investigation Unit). They have not been able to explain through use of logs how the customer credentials got leaked out. Further, they do not seem to have any monitoring system to alert about suspicious transactions. The Respondent in violation of Section 43A of the IT Act, and order them to a compensation of Rupees 1,30,000 (Rupees One Lakh Thirty Thousand) to the Complainant to partly cover his loss within a month of this

order, failing which compound interest of 12 percent compounded monthly will also be chargeable.

the case of **Sh. Chander Kalani, Smt. Romi Kalani Vs State Bank of India (Chief Manager, Linking Branch Road, Bandra,Mumbai) and others**[142]. It has been held that the complainant has been doing transactions with the banks only through emails, which is insecure way of doing things. Mechanisms like alternate email, SMS alerts etc. were not used. Complainant had not informed the bank about his defunct mobile number. Hence both the Complainant and the Respondent Bank have to share the blame.

The **Respondent No. 1 (State Bank of India)** in violation of Section 43A of the IT Act, and order them to a compensation of **Rupees 40,00,000 (Rupees Forty Lakhs)** to the Complainant to partly cover his loss, within a month of this order, failing which compound interest of 12 percent compounded monthly will also be chargeable.

Brief fact of the above case is: The complainants are Senior Citizens and Non Resident Indians having business in Lagos, Nigeria, West Africa. Complainants hold Joint NRE Account with SBI Respondent No. 1 bearing Account No. XXXXXXX0511. Complainants also hold Fixed Deposits Receipts (FDR) with Respondent No. 1.

The complainant had never opted for any services like transaction request through email/phone, Internet Banking facility or Phone Banking service form the Respondent.

The Complainants had Six Fixed Deposits with Respondent No 1 having different maturity dates and amounts. On 13th December 2013 when Complainant No 1 visited

[142] Sh. Chander Kalani, Smt. Romi Kalani Vs State Bank of India (Chief Manager, Linking Branch Road, Bandra,Mumbai) and others, Complaint No. 01 of 2014 dated 30th December 2013

Respondent No 1, to update their passbook and to collect one of the Original FDRs, he came to know that their FD were fraudulently transferred to some another account without his knowledge or his authorization. Respondent No 1, transferred the funds on the basis of the email received from complainant email ID XXXXXXIani@gmail.com.

Fraudster initiated email conversation with Respondent No 1 from 28th October 2013. Fraudster under the pretext of medical emergency, using complainant's email id, requested Respondent No 1 to transfer the amount USD 40000 immediately to another account in city of London. This account did not belong to the complainants. Respondent No 1 transferred GBP 60,000 which amounted to Rupees 63,00,000. Respondent No 1 even provided details to the fraudster about maturity dates of FDs of the complainants.

Email ID of the Complainant No 1, was compromised by fraudster enabling him to add filters to all the emails from Respondent No 1. Thus all emails from Respondent No. 1 were automatically deleted and never were shown in Complainant's Inbox.

Respondent was not diligent to cross check such fake emails with the complainants. Respondent even failed to take adequate Pre-transactions and Post-transactions measure related to fund transfer.

Respondent No 1 wrongly accepted scanned image of Form A-2 (which is mandatory in case of Foreign Exchange) which violates RBI mandates.

Complainant made a written complaint on 13th December 2013 to the Respondent No 1. On 18th December 2013, complainant lodged a police complaint with Khar Police Station.

Complainant is claiming damages Rupees 1,00,00,000 (Rupees One Crore).Complainant has paid application fee Rupees 2,03,260 through demand draft.

The suits for compensation that are brought up before the Consumer forums are at times required thorough examination of evidence and at times call for the lengthy process of examining of witnesses for its proper adjudication. Such powers are vested within the jurisdiction of the Civil Courts and the Forums not having such powers find themselves out of jurisdiction in sorting out the dispute. In such cases the matters are to be put before the competent Civil Courts.

State Consumer Disputes Redressal Comission, **Punjab in S.Harminder Singh Vs. IDBI Bank Ltd**[143] has rightly pointed out that the summary cases under the Consumer Protection Act are time bound and cases which require thorough examination of witnesses and leading elaborate evidence, both oral and documentary are rightly suited for the Civil Courts.

Brief facts of the case are as such: The appellant was having saving bank account No. 07210400042893 with respondent No. 2. On 12.11.2002, the balance in favour of the appellant was Rs. 1,52,087/- as per statement issued by respondent No. 2. Keeping this fact in mind, the appellant issued a cheque for a sum of Rs.14,500/- to one Sh. Rajwinder Singh on 27.11.2002, but the utter surprise of the appellant, this cheque bounced due to insufficient funds. The appellant approached respondent No.2 and demanded his account statement. Respondent No.2 issued the account statement to the appellant for a period up to 26.11.2002. the appellant noticed that a sum of Rs. 57,000/- had been withdrawn from his account through ATM transaction. The

[143] Punjab in S.Harminder Singh Vs. IDBI Bank Ltd, F.A. No. 1 of 2006 on 19th August 2011

appellant protested against these withdrawals as no ATM card had ever been issued to him till date. Thereafter, the appellant made regular visits to the respondents and requested for the reversal of these amount into his account but every time he was put off one pretext or the other. Hence the appellant filed a complaint for a direction to the respondent to credit a sum of Rs. 57,000/- into his account along with interest at the rate of 18% per annum from 26.11.2002 till realisation. He also prayed for compensation and costs.

The respondent filed written reply and contested the case. Apart from taking some preliminary objections, the respondents pleaded that earlier the appellant had opened a joint account in the respondent joint with bank jointly with *Gurjit Kaur* as co-applicant. But the said account was closed by the appellant on 20.12.2003 and on 14.1.2004, the appellant with joint applicant *Rajinder Singh* opened account vide account No. 07210400059255 and thus the complaint was liable to be dismissed on this score alone. It was further pleaded that ATM card and PIN number were duly received by the appellant. He had also operated his account through the ATM. The PIN code which was necessary for operating the card was supplied separately to the appellant and not along with ATM card. This procedure was supplied separately to the appellant and not along with ATM card. This procedure was followed in all ATM card cases, so as to avoid any chance of misuse or fraud.

It was also pleaded that the ATM card and separate PIN code numbers were also issued to Pawan Kaur daughter-in-law of the appellant as well as Gurjit Kaur wife of the appellant. On 23.11.2002 the account was operated through ATM at 8.30 PM which means that the ATM card and PIN code number had been rightly delivered to the accounts.

It was further pleaded that a family dispute was going on amongst the other family members in the police station. The present complaint had been filed by the appellant only to have an edge over the other family members. Hence dismissal of complaint was prayer.

After considering the pleadings of the parties and going through the documents on record, the learned District Forum vide impugned order dated 11.10.2005 dismissed the complaint of the appellant.

Hence the appeal by the complainant/appellant was made before the State Consumer Dispute Redressal Commission.

The submission of the learned counsel for the appellant was that the appeal be accepted, the impugned order dated 11.10.2005 passed by the learned District Forum be set aside and the respondents be directed to credit the amount of Rs.57,000/- in the account of the appellant and also pay compensation, interest and costs to him.

The submission of the learned counsel for the respondents was that there is no merit in the appeal and the same be dismissed. After the critical examination of the evidence placed on record and after hearing the submissions of both the parties the Learned Commission observed.

“The material question for determination by us is whether the appellant had withdrawn money from his saving bank account through the ATM card which the respondents have alleged to have to him.

As per the version of the appellant, the respondents had never issued any Atm card or PIN Code to the appellant and therefore, the question of the appellant having withdrawn any money from his account via the ATM transactions does not arise. The respondents on the other hand have proved the delivery report of Blue Dart Company

(Ex.R13) showing the delivery of the ATM card issued in the name of the appellant to one Shashi on 14.11.2002. the respondents have also pleaded that the PIN Code without which the ATM could not be operated was also sent to the appellant separately and not along with the ATM card so as to avoid any chance of misuse. However, no evidence has been led by the respondents to substantiate this version. The appellant has even denied having any relationship or concern with said Shashi let along the receipt of the ATM.

In our opinion, the decision of the present case requires determination of question of facts as to whether the appellant had opted for the ATM facility of respondent No.2 bank and whether the so called ATM card and PIN code which the respondents have alleged to have issued and sent to the appellant ever reached the hands of the appellant. Since these very facts are disputed between the parties, the affidavits and documents on record do not seem sufficient for the just adjudications of this case there is need for leading elaborate evidence both oral and documentary as well as examining of witnesses. Such an exercise, however, does not seem feasible in the time bound summary proceedings under the Consumer Protection Act,1986. As such we are constrained to hold that present case is not maintainable before us.

Resultantly, the appeal is dismissed with liberty to the appellant to seek his remedy before the Civil Court."

The judiciary through its various mechanisms have given a great contribution in resolving of matters of disputes between the banks and its customers regarding many of the menaces of the e-banking. Through the introduction of e-banking the banking world has been made more advance and easy to access. But with the same one has also become just a finger click away from being cheated from his hard earned money. ATM card frauds, frauds done through phishing and smishing and defects of the banks

while dealing and maintaining the account details have been reported through-out the country. The matters are heard and settled by various wheels and machineries of the Judiciary and has played a key role in upholding and meeting the ends of various legislations made for the purpose of tackling the menaces and hurdles on the path of e-banking.

The Judiciary has, through its various judgments, laid down various rules and regulations to be followed by banks and customers to ensure safe and protected use of their personal accounts. The Judiciary through its various judgments upon dealing with the frauds arising out of Phishing and Smishing, ATM and debit card frauds have laid down for the importance of not sharing the details of ones account with other individuals.

CHAPTER - VII

7. CONCLUSION AND SUGGESTIONS

The Internet has grown exponentially in this society. The interaction between two businesses as well as between individuals and businesses were increased by the internet. With the development of the Internet, electronic commerce has emerged and offer wonderful market potential for today's businesses. The banking industry is one of the industries which gained benefits from this new communication channel. Banking customers are getting a wide variety of services which is provided by electronic banking such as customers get easy interaction with their bank accounts as well as make financial transactions from anywhere at any time through internet.

In today's world, economy totally depends upon banking; hence it is known to be the backbone of an economy. With the introduction of internet banking, the era of internet banking has come to the verge of conclusion. As the transaction can be done with the click of the button it is a time saver, people do not have to stand in line for long hours in the bank to do their work, therefore it has proved to be more convenient for the people than the traditional way of banking. However, its intangible nature has created fear amongst the common people. The whole process of internet banking depends upon the users trust. In the early years of 1990s India introduce the new economy policies, which liberalized into the world economy. With the introduction of Internet banking by the ICICI bank, the protection for the customer's accounts from cyber crime was also introduced as there was no appropriate law. Therefore, in 2000 the Indian Government passed the Information Technology Act. This Act provides the provisions for the protection of cyber crime. However, with these Information Technology Act people were not convinced to use internet as their way of banking.

In 2008 the Indian Government passed the Information Technology Amendment Act which amended many provisions such as; in the principle Act section 3, sub-section (4)&(5) were added and also section 3A has been inserted. With the introduction of Information Technology Amendment Act, 2008, the Reserve Bank Of India made their internet Banking Guidelines, such as; Master Circular on Know Your Customer (KYC)[144], Internet Banking in India- Guidelines[145], Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations[146] etc. with this Amendment Act, many banks emerged successful from the technical changes. Information Technology has become the most precious and important tool in today's world. With the help of Information Technology the economy has been liberalized into the whole world. As Information technology renders or stores data, information, and knowledge in a form of visual format, the people do not have to keep in mind the whole thing. We can open the data whenever needed, as it has already been stored.

However, India has a long way to compete globally, due to the lack and late introduction of Information Communication Technology (ICT). In India ICT was first introduced in 1991, if the ICT would have been introduced in India a little early, the internet banking would also have been introduced early. India also lacks in better equipments, newer forms of services and dynamic environment. Technology gives the bank, the opportunity to be closer to the customers in a vary board range of services at lower cost, and streamline the systems which leads to the new products. Internet banking means anyone or any users with a device such as personal computer, mobile, laptop or any other electronic device that connects through internet and has an internet

[144] RBI Vide Circular DBOD. AML. BC. No. 11/14.01.001/2012-13)

[145] Vide RBI Circular, DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01, June 14, 2001.

[146] RBI/2010-11/494 DBS.CO.ITC.BC.No. 6/31.02.008/2010-11

connection can get linked to his bank account through bank website to perform any of the internet banking functions.

There are two concept of internet banking: (i). In internet banking, if operation are conducted exclusively over the internet without the use of any physical offices, and (ii). The other has offices but has no distribution channels for services to the consumers. India still is, at early stages of internet banking and its growth and development. Internet banking means a lot more than just going paperless, it offers a new improved and better customer experience and are capable of delivering faster and efficient services. Moreover internet banking is called online banking as its channel is internet.

With the use of Automated Teller Machine, telephone banking, direct bill payment, Electronic Fund Transfer, the era of internet banking has began. Internet banking is very beneficial and advantages for the bank and their clients as, it are a time sever, reduces the cost, achieves new segments of the society, effectiveness and improves bank status. It is widely recognized that internet banking provides more revenue per customers and costless, per transaction. In contrast, due to the intangible nature of banking, the concept of trust is vital consideration in online banking because the customers get involved in financial activities and these are considered about shearing their essential file and important information like pin code, password, account number and personal information etc.

After independent of India in 1947 Indian Banking system has travelled a long way facing ups and down in the economy, such as time-consuming business establishment to an extremely practical and dynamic entity. To increase the pace of computerization in the operation of banking sector, Reserve Bank of India was set up two committees in early 1980s. The first committee introduce computerized section and mechanized

sections in the banking sector. And the committee introduced a plan for automation to other areas like Email, ATNs etc.

In today's market economy, the three types of internet banking are being used; they are; (i) informational, (ii) communicative and (iii) transactional. Reserve Bank of India has a duty to issue appropriate directions such as; guidelines, Secure Socket Layer that protects the transaction from the third party users etc. for the bank operation and they have been issuing various directions and recommendation from time to time to strengthen cyber security for the banks operating in India. After that Digital India Programme was launched on **1 July 2015** by Prime Minister Narendra Modi. The initiative includes plans to connect rural areas with high-speed internet networks. Digital India consists of three core components such as digital infrastructure as a core utility to every citizen, governance and services on demand, digital empowerment of citizens. To implement this mission in banking sector, on 8^{t-h} November 2016 by our Prime Minister *Narendra Modi* has announced that the demonetization of 500 and 1000 rupee note.

In last 10 years, information technology has brought significance changes in the banking sector. Apart from business operation, development in technology has played a crucial function in the distribution channel of commercial banks. A part of planned decisions banks in India have been spending a lot of money on computer and a related technologies expecting sustainable pay off. In 2011 the expenditure of information technologies for bank was 2.7% per annum of their total revenues that contributes sum of total 6.500 cr. Further it is likely to increase up to 10 thousand cr. annually.

The abolition of internet banking has transformed the way of bank traditionally conducted their businesses. Today internet banking has rapidly increasing and it has become the main mode for delivering banking product and services. However, internet

banking has the risk of cyber crime such as; hacking, phishing, vishing, denial of service attack etc. Therefore, in the view of these Indian banking has introduce a pre-login and post security features and privacy features in which it is used in the internet banking services. A customer has given user ID and password by the banks at the time of opening an account as a part of welcome kit, to login to his account.

Another feature of internet banking is virtual key. It secures the websites from key loggers, as the customer has to enter authentication details. Recently in order to maximize the security two more forms are added "Scrambled Keyboard'' and "Hovering keyboard". Even though from the beginning of the world the number of days in a year has remained the same, the people now days are so busy in their day to day activities that they do not get ample time to complete their work. Therefore in this busy world the way of traditional banking is just a waste of crucial time, as the customers has to stand in the bank in line for a long hours, until their turn comes.

Since the introduction on internet banking or otherwise called as online banking in the early 80s, it appears to be the boon for the people, as many of the people have benefited from these facilities. Online banking appears to be a source for time saver for the people. However, when online banking became popular in the late 1980s it used to have a very different meaning than it does today. When the four major banks of United States i.e., Citibank, chase *Manhantton*, Chemical Bank and Manufactures Hanover used online banking system to provide home banking services to their customers, by use of terminal, keyboard, television, and computer monitor to access one's bank account using a telephone, was defined as online banking. Whereas in today's world the online banking or internet banking is defined to anything that includes electronic payment system that allows customers of a financial institution to

conduct financial transactions, it also includes mobile internet banking technologies, such as person-to-person payment applications and text banking.

By the 2000 online banking had become the mainstream for banking as it gained popularity in e-commerce too. When the big banks began to offer online products and services, internet banking gained legitimacy for consumers. An overwhelming 80 percent of the banks in the United States along were offering internet banking services. In 2001 Bank of America made history as it became the first financial institution to gain more than 3 million banking customers.

In United States there is a medium of legislation and regulation hat specifically codifies the use of rights associated with the internet and e-commerce in general, and the electronic banking and internet banking activities. The international model laws promoted the guidance to the member nations on the necessity for revising existing legal structures to accommodate electronic transitions. The important laws for general application to commercial activity over the internet are as follows-

(i) Uniform Commercial Code

(ii) The Uniform Electronic Transitions Act

(iii) The E-sign Act and

(iv) The Gramm Leach Bliley Act.

Almost simultaneously with the United States online banking arrived in the United Kingdom. The first electronic banking service was introduced in the Nottingham Building Society Britain in the year 1983. The United Kingdom's first online banking services were known as Home-link which was setup by the bank of Scotland for the customers. As they found the procedure of identification of new customers proper can

lead to the serious risks for the banks, they also made important laws for general application, such as;

(i)Data Protection Act (ii) The Computer Misuse Act.

Internet banking in Australia is categorized into two forms;

(i)Web Based and

(ii)Provision of Proprietary Software

The initial web based products have focused on personal banking whereas the provision of proprietary software has been targeted at the corporate sector.

In India internet banking is recently originated. The traditional banking has been through branch banking. The rigorous use of Information Technologies in the banking sector started immediately after the recommendations of the committee on the Financial System in 1991.The credit of launching internet banking goes to ICICI Bank. Later in 1999 Citibank and HDFC followed the internet banking services. Several initiatives were taken by the government of India along with Reserve Bank of India. The government of India enacted the Information Technology Act in 2000, which provided legal recognition to electronic transitions and other means of electronic commerce. The Reserve Bank is the main body which supervises and reviews the legal and other requirements of internet banking on a continuous basis for the development of internet banking on solid lines and e-banking related challenges would not pose a threat to financial stability. Further, a secure mode of transferring funds from one branch bank to the other branch bank was introduced to be known as National Electronic Fund Transfer (NEFT).

During the past decade, there has been observed that, in the banking and financial organisation has a significant change to conduct banking businesses and provide their

product and services to their customers. This change has happened because the banking industries were implemented information technology in the core functions of the business. However, information systems and the internet banking businesses have been facing verity of security threats from a wide variety of sources including computer-assisted fraud, espionage, sabotage, vandalism etc[147]. There are various types of damage which have become more common in the internet banking environment, such as the computer viruses, computer hacking, phishing, denial of service attack, card skimming etc. The ever-growing reliance of banks on the information systems has made them more susceptible to such security threats. This has made it vital for every bank to put adequate security controls measures to certify data accessibility to all the authorized users and data inaccessibility to all the unauthorized users as well as maintenance of data integrity.[148]

There are various legal, security and privacy issues in i-banking services, such as; (i). Problem relating to online opening of account- RBI provides guidelines to all banks for opening an account through Internet, account which says it should be opened only after proper introduction and physical verifications of the identity of the customer but private banks are not following the guidelines properly in order to raise their business they are opening an account without the proper verification of customers identity. This amount to non-compliance of the RBI directive "Know Your Customer" and makes the whole system vulnerable to attacks. (ii). Problem of authentication as well as banks in India lag in security of card transactions- Second major problems faced by banks

[147] RBI Reports on Information Systems Security Guidelines for the Banking and Financial Sector (Part 1 and 2) dated: 11 Mar 2002, online available at https://www.rbi.gov.in accessed on 22nd oct. 2016.

[148] Dr. Tejinderpal Singh, *"Security and Privacy Issues in E-Banking: An Empirical Study of Customers' Perception",* A Micro Research Project Report (2012-2013).

involved in internet banking is the issue relating to authentication as well as banks in India lag in security of card transactions. The present legal regime does not set out the restrictions as to the extent to which a person can be bound in respect of an electronic instruction purported to have been issued by him. Generally, authentication is achieved by security procedure. Methods and device like the relationship numbers, telephone-PIN numbers, and personal identification numbers (PIN), code numbers, passwords, account numbers and encryptions are developed to set up authenticity of an instruction. Security issues are important because these fraudsters can become serious to an individual in his life. One can be a victim of a cyber crime in several ways. Against the background of well known global cases of card breaches, the banks in India have not been adopted that the basic measures for ensuring card security. (iii). Liability of banks in bilateral agreement- The definition of consumer and provisions for rights and liability of the customers has been provided under Consumer Protection Act, 1986 thus banking customers are also comes under this Act, therefore the provision of the Act are also applicable to banking services as well.[149] The rights and liabilities of both the banks as well as customers are determined by the bilateral agreement between banks and customer. Sometimes the agreement contains the provisions which are contrary to the consumer's interest. In such a situation whether any agreement between bank and customer defining customer's rights and liabilities which are adverse to consumers than what is enjoyed by them in the traditional banking scenario will be legally tenable? Also in case of unauthorized hacking how the liability in such a situation will be determined. Further in case of denial of service also. Although the Information technology Act contains the provision of penalty for denial of access to a computer system(s-43) and hacking (s-66), but when it comes to

[149] Source available at https://www.ukessays.com/essays/information-technology/regulatory-and-supervisory-issuesinformation-technology-essay.php

the determine the liability of banks the Act gives no clue. (iv). Problem relating to privacy and confidentiality of customer account and inadequacy of data protection law- It is a duty of banks to maintain privacy and confidentiality of the customer's account, but in internet banking, banks obligations to maintain privacy and confidentiality is very difficult task because hackers can operate others account, but bankers are not in a position to trace them. They come to know only when the customer informs them of some irregularity in their transaction. The banks are lacking instituting adequate risk control measures to manage such risk. Internal management systems of banks are also not fully gear for the digital age. And adequate risk control measures are not apposite in India. It is impossible for banks to retain information solely within their own computer networks, let alone a single jurisdiction of data is sufficiently high. Banks are deficient in providing adequate legal and technical protection. (v). Cyber Security of Banks in India Needs Strengthening- The Information Technology Act, 2000 (IT Act,2000) is the sole cyber law of India. However, it is not capable of forcing the companies and individuals to disclose cyber security breaches and cyber crimes. Nevertheless, the rules under IT Act, 2000 prescribe cyber law due diligence, internet intermediary, reasonable cyber security practices etc. They indirectly cover some aspects of cyber security discloser norms. But they are not sufficient to meet the demand of present time. Some basic level guidelines and recommendation have been issued by RBI but they are far from satisfactory and being effective. RBI has also mandated establishment of Steering Committees on Information Security by Banks in India and appointment of Chief Information Officers (CIOs) for all banks in India. However, banks in India have failed to comply with the directions of RBI so far and even RBI has allowed them to take liberty. In effect, this means that there is neither a legal framework nor any

compulsion to ensure cyber security of banks in India. Naturally, the online banking system in India is not at all cyber secure and banks in India are not following cyber security due diligence and cyber law due diligence at all.

Branch Banking is regulated by set of enactment like the Banking Regulation Act, 1948, the Reserve Bank of India Act, 1949 and the Foreign Exchange Management Act, 1999. Apart from these, banking businesses were also influenced by several legislations governing trade and commerce, i.e., Indian Contract Act, 1872, the Negotiable Instruments Act, 1881, Indian Evidence Act, 1872, Bankers Books Evidence Act, 1891, etc. Internet banking is an expansion of the branch banking, hence, various provision of law, which are related to branch banking activities, are also applicable to internet banking. However, use of electronic medium in general and internet in particular in banking transactions, has put to question the legality of certain types of transactions in the context of existing statute. The validity of an electronic message/document authentication, validity of contract entered into electronically, non-repudiation etc. is important legal questions having banking on electronic commerce and internet banking. The vulnerability of data/information passing through internet has also raised the issue of ability of banks to comply with legal requirement practices like secrecy of customers account, privacy, consumer protection etc.. There is also the question of adequacy of law to deal with situations which are technology driven like denial of services/data corruption because of technological failure, infrastructure failure, hacking, etc. Cross border transactions carried through internet pose the issues of jurisdiction and conflicts of laws of different nations. Therefore, the Reserve Bank of India has issued various internet banking guidelines for the protection of cyber crime such as; Internet Banking in India- Guidelines, **Guidelines on electronic payments security transactions.**

The judiciary through its various mechanisms have given a great contribution in resolving of matters of disputes between the banks and its customers regarding many of the menaces of the internet banking. Through the introduction of internet banking the banking world has been made more advance and easy to access. But with the same one has also become just a finger click away from being cheated from his hard earned money. ATM card frauds, frauds done through phishing and smishing and defects of the banks while dealing and maintaining the account details have been reported through-out the country. The matters are heard and settled by various wheels and machineries of the Judiciary and has played a key role in upholding and meeting the ends of various legislations made for the purpose of tackling the menaces and hurdles on the path of internet banking.

The area of this research is to analysis the security and legal issues of internet banking as well as legal framework for the regulation of internet banking within India with comparison to other develop country.

And the findings of the study are that internet banking has various kinds of security threat or cyber fraud. To protect such types of security threat banks are not adopting the well developed technology as having UK and USA. And to protect the cyber crime relating to internet banking such as ATMs fraud, hacking etc., are IT Act, 2000, but there was no single provision for data protection. But in 2008, Indian Parliament amend the IT Act and incorporate few small provisions for the protection of computer data but this Act of Legislation are not adequate to tackle the emerging issues of internet banking.

The hypothesis of this research is "**In internet banking there are various legal & security issues but the regulatory framework to deal with is very weak**". And it is

proved that the legal framework of India is not enough to regulate the various issues of internet banking in India.

Lastly, In order to reduce the potential vulnerabilities regarding to the security, many vendors have developed various solutions in both software-based and hardware-based systems. Generally speaking, software-based solutions are more common because they are easier to distribute and are less expensive. In order for internet banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard.

7.1 SUGGESTION

1. Information Technology Act passed in the year 2000 based on UNCITRAL Model Law of E-commerce, but there was no provision given on data protection. But in 2008, Parliament amend the IT Act and incorporated few small provisions for the protection of computer data by services providers but this provision are not adequate to tackle the serious issues of internet banking. Hence there is a need to pass a separate law containing various provisions of data protection liabilities as UK having.

2. Banks should create awareness among people about internet banking products and services. Customers should be made literate about the use of internet banking products and services.

3. Special arrangements should be made by banks to ensure full security of customer funds and privacy. Technical defaults should be avoided by employing well trained and expert technicians in the field of computers, so that loss of data can be avoided.

4. Employees of banks should be given special technical training for the use of new technology so that they can further encourage customers to use the same.

5. Seminars and workshops should be organised on the healthy usage of internet banking especially for those who are ATM or computer illiterate.

6. Internet banking services should be customized on the basis of age, gender, occupation etc. so that needs and requirements of people are met accordingly.

7. Government should make huge investments for building the infrastructure and should pass much appropriate legislation for security issue on internet banking, for the protection of customers' interests.

REFERENCES

1. BOOKS

i. Reed, Chris (2010), *"Internet Law",* Published by Universal Law Publishing Co. Pvt. Ltd., second edition.

ii. Gemoz, Clifford (2011), *"Banking and Finance Theory, Law and Practice",* New Delhi, published by PHL Learning Pvt. Ltd.

iii. Lloyd, Ian J. (2011), "*Information Technology Law",* published by Oxford University Press, seventh edition.

iv. Justice Singh, Yatindra (2010), *"Cyber Laws",* Published by Universal Law Publishing Co. Pvt. Ltd., fourth edition.

v. Parthasarathy, M. S. (2003) *"Cheques in Law and Practice",* published by Universal Law Publishing Co. Pvt. Ltd., edition sixth.

vi. Gupta, S. N. (2007), *"Supreme Court on Banking Law",* Published by Universal Law Publishing Co. Pvt. Ltd. Fifth edition.

vii. Tannan M.L. (2010), "*Banking Law and Practice in India"*, Nagpur, Lexis Nexis Butter Worths Wadhaw.

viii. Cranston, Ross (2008), *"Principles of Banking Law",* Published by Oxford University Press, Second Edition.

2. ARTICLES

i. French, Aaron M. (2012), "A Case Study on E-Banking Security- When Security Becomes Too Sophisticated for the Access Their Information", *Journal of Internet Banking and Commerce,* Volume. 17, No.28.

ii. Boon & Yu Ming Cheng (2003), "Success Factors in E-channel, the Malaysian Banking Scenario", *International Journal of Bank Marketing*, Vol. 21, No. 6/7

iii. Ceren & Simon, "Internet Banking Market Performance: Turkey Versus the UK", *International Journal of Bank Marketing,* Vol.25 Issue 3.

iv. Chou &Chou, (2000), "A Guide to the Internet Revolution in Banking", *Information System Management,* Vol. 17, No. 2.

v. Shen Chiou (2012), "The antecedent of online financial service adoption: the impact of physical banking on internet banking acceptance", *Behaviour and Information Technology*.

vi. Daniel E., "Provision of electronic banking in the UK and the Republic of Ireland", *International Journal of Bank Marketing*.

vii. Flavian, Carlos and Guinalu, (2006), "How Brick-and-Mortar attributes affect online banking adoption", *International Journal of Bank Marketing,* Vol. 24, No. 6.

viii. Gerrard, Philip, Cunnighan, Barton, Devlin & James (2006), "Why Consumers are not Using Internet Banking: A Qualitative Study", *Journal of Service Marketing,* Vol. 20, No.3.

ix. Gunajit Sharmaa & Pranav Kumar Singh, *Ïnternet Banking: Risk Analysis and Applicability of Biometric Technologies for Authentication",* International Journal of Pure and Applied Science and Technology, 1(2).

x. Kesharwani, Ankit and Bisht, Shailendra (2012), "The Impact of trust and perceived risk internet banking adoption in India: An extension of technology acceptance model", *International Journal of Bank Marketing,* Vol.30, No. 4.

xi. Pooja and Balwinder (2007), "Determinants of Internet Banking Adoption by Banks in India", *Internet Reserch,* Vol.17, No. 3.

xii. Nelson & Queenie (2006), "Consumer Attitudes, System's Characteristics and Internet Banking Adoption in Malaysia" *Management Research News,* Vol. 29.

xiii. N. M. Gaikwad & A. U. Charumathi (2013), "Impact of Information Technology Investment on the Cost Efficiency of Indian Banking Sector- A Stochastic Frontier Approach", *International Journal of Engineering & Technology*, Published by (c) Maxwell Scientific Organisation.

xiv. Sarel & Marmorstein (2003), "Marketing Online Banking Service: The Voice of the Customer", *Journal of Financial Service Marketing,* Vol. 8 No. 2.

xv. Sathye, Milind (1999), "Adoption of Internet Banking in Australian Consumers: an empirical investigation", *International Journal of Bank Marketing,* Vol. 17, No. 7.

xvi. Singh Tejinderpal, Kaur Manpreet (2012), "Internet Banking: Content Analysis of Selected Indian Public and Privte Sector Banks", Vol. 17, No. 1,.

xvii. S. T. & B. Charumathi (2013), "Impact of Information Technology Investment on the Cost Efficiency of Indian Banking Sector- A Stochastic Frontier Approach", *International Journal of Engineering and Technology*.

3. INTERNET

i. *RBI report on Internet Banking (22 jun 2001)* online available at https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243, accessed on 19the March 2016.

ii. *RBI Publication on operation and Performance of Commercial Bank on 8th Nov. 2012,* source available at www.rbi.org.in/scripts/PublicationsView.aspx?id=14629, accessed on 27th March 2016

iii. Dr. Suresh & M. P. Chandrika, *"Law Relating to E-banking in India- An Outreach Challenges",* online available at http://jsslawcollege.in/wp-content/uploads/2013/05/LAW-RELATING-TO-E-BANKING-IN-INDIA-%E2%80%93-AN-OUTREACH-CHALLENGE.pdf. "Digital India: Opportunities Beyond Imagination", online available at mobilityindia.com accessed on 29th Nov. 2016.

iv. Deepshika Jamwal & Devanand Padha, *"Internet Banking System in India: Analysis of Security Issue",* source available at http://www.bvicam.ac.in/news/INDIACom%202009%20Proceedings/pdfs/papers/80.pdf. accessed on 25th Oct. 2016

v. *"Digital India: Opportunities Beyond Imagination",* source available at http://www.pwc.lu/en/press-articles/2012/banking-will-mean-digital-banking-in-2015.html., accessed on 19th March 2016.

vi. *"Final Study of Internet Banking in India",* source available at http://www.slideshare.net/Dharmikpatel7992/final-study-of-internet-banking-in-india-2427., accessed on 29th Sept. 2016.

vii. http://www.syndicatebank.in/scripts/financialinclusion.aspx. accessed on 14th Sept. 2016.

viii. *"India is first country to give discounts on online payment",* online available at www.daytodaygk.com accessed on 29th Nov. 2016.

ix. *"Internet Banking- Legal Issues",* online available at www.rajdeepandjoyeeta.com/**internet-banking**.html, accessed on 14th Dec. 2016.

x. *"Internet Banking in India",* source available at http://www.tips.thinkrupee.com/articles/internet-banking-in-india-php., accessed on 3rd Sept 2016.

xi. *"Legal Framework of E-Banking services"* online available at http://shodhganga.inflibnet.ac.in:8080/jspui/bitstream/10603/54288/10/10_chapter%204.pdf, accessed on 3rd Sept. 2016.

xii. *"Modern Information"* online available at https://www.coursehero.com/file/po189u/First-Existing-Customers-may-become-Former-Customers-eg-decide-to-buy-from-a/ accessed on 29th Nov. 2016.

xiii. *"RBI Publication on Operation and Performance of Commercial Bank on 8th Nov. 2012"* online available at www.rbi.org.in/scripts/PublicationsView.aspx?id=14629 accessed on 29th Nov. 2016

xiv. Singh, Dr. Tejinderpal (2012-2013), *"Security and Privacy Issues in E-Banking: An Empirical Study of Customers' Perception",* Micro Research Project Report (2012-2013), online available at http://iibf.org.in/documents/reseach-report/Tejinder_Final%20.pdf, accessed on 27th July 2016.

xv. www.digitalindia.gov.in/content/introduction, accessed on 16th Aug. 2016.

xvi. Alam Tanvir, *"Marketing strategy of digital marketing: a comoarative study of five companies in Bangladesh",* online available at www.academic.edu, accessed on 29th Nov. 2016.

xvii. Vincent Villers, *"Banking will mean digital banking in 2015",* Press releases on jan. 2015, online available at http://www.pwc.lu/en/press-articles/2012/banking-will-mean-digital-banking-in-2015.html, accessed on 25/04/2016

xviii. Yi-Jen Yang, *"The Security of Electronic Banking"*, online available at csrc.nist.gov/nissc/1997/proceedings/041.pdf, accessed on 25th July 2016.

xix. Zakaria, Mohammed & Aliar (2009), *"Towards Secure Information System in Online Banking".* Online available at https://www.researchgate.net/publication/224110362_Towards_secure_information_systems_in_online_banking accessed on 25th November 2016.

4. ACT and GUIDELINES

i. Banking Regulation Act, 1949

ii. Foreign Exchange Management Act, 1999

iii. Information Technology Act, 2000

iv. Information Technology Amendment Act, 2008

v. Reserve Bank of India Act, 1934

vi. Credit Information Companies (Regulation) Act, 2005

vii. Internet Banking guidelines issued by RBI

1. Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA), 2002 (RBI Vide Circular DBOD. AML. BC. No. 11/14.01.001/2012-13)

2. Internet Banking in India- Guidelines (Vide RBI Circular, DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01, June 14, 2001.)

3. Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations, (RBI/2010-11/494 DBS.CO.ITC.BC.No. 6/31.02.008/2010-11)

viii. Indian Contract Act, 1872

ix. Indian Evidence Act, 1882