CYBER FRAUDS IN THE INDIAN BANKING INDUSRTY: A CRITICAL LEGAL STUDY

Dissertation submitted to National Law University, Assam

in partial fulfillment for award of the degree of

MASTER OF LAWS

Supervised by

Dr. Thangzakhup Tombing

Assistant Professor of Law

Submitted by

Dibyasri Hazarika

UID- SF00220009

2020-21, II Semester

National Law University, Assam

2021

NATIONAL LAW UNIVERSITY AND JUDICIAL ACADEMY, AMINGAON, ASSAM - 781031

CERTIFICATE

This is to certify that the dissertation entitled **"CYBER FRAUDS IN INDIAN BANKING INDUSRTY : A CRITICAL LEGAL STUDY"** submitted to National Law University And Judicial Academy, Assam is a bonafide study conducted by **Dibyasri Hazarika** as a requirement for the completion of the course for the Master of Laws (LL.M) degree under my constant guidance and supervision.

This is also certified that she has fulfilled all the regulations and requisite of National Law University And Judicial Academy, Assam for preparing and completing a dissertation for Master Degree in Laws.

With the authority as her guide and the Associate Professor of Law, the dissertation is hereby recommended for submission and onward proceedings as per regulation.

Date:

Place : Guwahati

(Dr. Thangzakhup Tombing)

Assistant Professor of Law

NATIONAL LAW UNIVERSITY AND JUDICIAL ACADEMY,

AMINGAON, ASSAM - 781031

DECLARATION

I hereby declare that, this dissertation titled **"CYBER FRAUDS IN INDIAN BANKING INDUSRTY : A CRITICAL LEGAL STUDY"** is a bonafide and genuine research work carried out by me under the guidance of **Dr. Thangzakhup Tombing, Assistant Professor of Law, National Law University and Judicial Academy, Amingaon, Assam.**

I further declare that to the best of my knowledge the dissertation does not contain any part of work, which has not been submitted for the award of any degree either in this University or any other institutions without proper citation.

Date :

Place : Guwahati

Dibyasri Hazarika

LLM

National Law University and
Judicial Academy, Assam

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I am highly indebted to Hon'ble Vice Chancellor Prof. Dr. V. K. Ahuja Sir for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

I would like to thank our guide Dr. Thangzakhup Tombing, Assistant Professor of Law, National Law University and Judicial Academy, Assam, for his constant support, help, motivation, guidance and valuable suggestions throughout the period of this study, will always be fondly remembered as an affectionate teacher and guide who is a constant source of inspiration. I will be forever grateful for his kind and friendly behavior.

I would like to express my gratitude towards my parents for their kind co-operation and encouragement which help me in completion of this seminar. Also I would like to express my gratitude towards my friends specially Adv. Tanay Paul (ex student of NLUJAA, Batch 2019-20, specialization in corporate law) for his constant support, guidance, help and encouragement.

I express my sincere thanks and gratitude to Dr. Kankana Baishya, Assistant Librarian, National Law University and Judicial Academy, Assam and the Library Section for their invaluable help in carrying out my dissertation study.

Above all I would also like to express my sincere gratitude to all authors whose precious writings have been utilized in my study and those provided their valuable information and insights during my seminar.

Last but not the least I submit to the GOD without whose blessings this endeavor would not have been possible.

Dibyasri Hazarika

UID SF0220009

LL.M (2020-2021)

TABLE OF ABBREVIATIONS

1.	ALPMs	ADVANCED LEDGER POSTING MACHINES
2.	ATM	AUTOMATED TELLER MACHINE
3.	BHIM	BHARAT INTERFACE FOR MONEY
4.	CBI	THE CENTRAL BUREAU OF INVESTIGATION
5.	ECS	ELECTRONIC CLEARING SYSTEM
6.	ECS	ELECTRONIC CLEARING SYSTEM
7.	EDI	ELECTRONIC DATA INTERCHARGE
8.	FEI	FINANCIAL EXECUTIVE INTERNATIONAL
9.	FEMA	FOREIGN EXCHANGE MANAGEMENT ACT
10.	FS-ISAC	FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER.
11.	FIU-IND	FINANCIAL INTELLIGENCE UNIT INDIA
12.	FY	FINANCIAL YEAR
13.	IBA	INDIAN BANK EMPLOYEE ASSOCIATION
14.	ICT	INFORMATION AND COMMUNICATION TECHNOLOGY
15.	IEA	INDIAN EVIDENCE ACT, 1872
16.	IT	INFORMATION TECHNOLOGY
17.	IIT	INDIAN INSTITUTE OF TECHNOLOGY
18.	IAMAI	THE INTERNET MOBILE ASSOCITION OF INDIA
19.	IDRBT	INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY
20.	IT ACT	INFORMATION TECHNOLOGY ACT
21.	IPC	INDIAN PENAL CODE
22.	ISTF	INFORMATION SECURIYT TASK FORCE

23.	HSBC	HONKONG AND SANGHAI BANKING CORPORATION LIMITED
24.	LPG	LIBERALIZATION, PRIVATIZATION AND GLOBALIZATION
25.	MICR	MAGNETIC INK CHARACTER RECOGNITION TECHNOLOGY
26.	NPA	NON-PERFORMING ASSESTS
27.	NPCI	NATIONAL PAYMENTS CORPORATION OF INDIA
28.	NCSIA	NON CONSENSUAL SHARING OF INTIMATE IMAGE
29.	NCRB	THE NATIONAL CRIME RECORDS BUREAU
30.	NI ACT	NEGOTIABLE INSTRUMENT ACT
31.	OTAS	ONLINE TAX ACCOUNTING SYSTEM
32.	PC	PERSONAL COMPUTER
33.	PDA	PERSONAL DIGITAL ASSISTANT
34.	PIN	PERSONAL IDENTIFICATION NUMBER
35.	PSB	PUBLIC SECTOR BANKS
36.	RBI	RESERVE BANK OF INDIA
37.	RBI ACT	RESERVE BANK OF INDIA ACT, 1934
38.	RTGS	REAL TIME GROSS SETTLEMENT
39.	ReBIT	RESERVE BANK INFORMATION TECHNOLOGY PRIVATE LIMITED
40.	SMS	SHORT MESSAGE SERVICE
41.	SEC	SECTION
42.	SPNS	SHARED PAYMENT NETWORK SYSTEM
43.	UNCITRAL	THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

44.	UPI	UNITED PAYMENT INTERFACE
45.	UNCTAD	UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT
46.	UNTOC	UNITED NATIONS CONVEN ORGANIZE CRIME
47.	VPN	VIRTUAL PRIVATE NETWORK
48.	WFH	WORK FROM HOME
49.	WHO	WORLD HEALTH ORGANIZATION
50.	WTO	WORLD TRADE ORGANIZATION

LIST OF STATUTES

1. 2000 – The Information and Technology Act
2. 1860 – Indian Penal Code
3. 1891 – The Bankers' Book Evidence Act
4. 1961 – Income Tax Act
5. 1981 – Negotiable Instrument Act
6. 2001 – Prevention of Money Laundering Act
7. 1980 – Consumer Protection Act

LIST OF CASES

CONTENT

CHAPTER 1

1.1. INTRODUCTION

The new millennium is experiencing a new online culture, or a digital revolution, that drastically transformed our way of life. The internet offers immense potential for transmitting knowledge beyond geographical boundaries due to its speed, interactivity, and diversity. Without a doubt, the digital revolution or new internet culture has altered people's lifestyles, particularly in urban regions. In today's era of tremendous expansion of "Information Technology (IT)" is affecting the day to day life of all people in every corner of our society. The paperless proceedings have been made feasible, thanks to technical advancements. We are currently setting new norms for communication pace, competence, and perfection, which have become critical instrument for improving innovation, creativity, and overall productivity. Computers are often utilized to store sensitive data of a political, social, economic, or personal nature, which benefits society greatly.[1]

Globalization ushered a new era and with the rapid growth of information technology and internet, banking industry hopped on to this internet culture too. The banking industry has drastically changed over the years and it introduced "internet banking" or "e-banking" to the world which has been revolutionized. Internet banking which is often known as online banking has transformed a key activity in the twenty-first century. With the advancement of e-banking technology, the work has become much easier, and banking transactions may now be completed in a matter of seconds.[2] Daily banking is made easier and faster with online and mobile banking. Misuse of information technology in cyberspace is on the rise, giving rise to cyber crime on a national and international scale. However online and mobile banking is never 100 per cent safe. The proportion of dangers and obstacles associated with it has risen.

With its inherent benefits for both the banking sector and the client, electronic banking is an area with significant growth potential. "Network Security Breaches,

[1] Akram Jalal & Jasim Marzooq & Hassan A. Nabi, 'Evaluating the Impacts of Online banking Factors on Motivating the Process of E-banking' (2011) 1 J Mgmt & Sustainability 32

[2] Naser Asgari and Mohamad Hassan Ahmadi and Mehdi Shamlou and Atefe Rashid Farokhi and Milad Farzin, 'Studying the Impact of E-Service Quality on E-Loyalty of Customers in the Area of E-Banking Services' (2014) 4 J Mgmt & Sustainability 126

Data Thefts, Data losses, Identity Thefts, and Other White Collar Crimes" have all increased in this field, resulting in massive losses for the banking industry. The banking industry has suffered massive losses as a result of white collar crimes all across the world, far outnumbering traditional tactics of bank robbery. The rapid evolution of online banking, the pervasiveness and worldwide character of open networks, and our excessive dependency on technology have all combined to create a platform for greater issues related to securities. Amendments to the "Information Technology Act (IT)", banking laws, and numerous wireless networking challenges all need to be considered by the industry. [3]

An assault could come from anywhere if a computer system of a bank is connected to the "internet" or "intranet". Before commerce can be reliably performed on the internet, some level of security must be established. Unauthorized access, data loss, corruption, or alteration, or any type of malicious procedure to cause network failure, reboot or hang, are all examples of attacks. Cracking has become more difficult, but not impossible, thanks to modern security methods. Furthermore, if the system is not configured properly or current patches are not implemented, hackers may exploit a security flaw to get access to the system. [4]

Technology has made our lives easier; but, there is a risk of cyber fraud as a result of its misuse. The use of online transactions, digital data transfer, electronic databases, and a variety of other business, social, and other activities based on computers, the internet, and information technology tools has become increasingly popular around the world. Many innocent people are victims of cybercrime all throughout the world. When confidential information is unlawfully lost or disrupted, high-profile crimes such as cyber terrorism, financial theft, copyright infringement, hacking, and so on result. Cybercrime is on the rise every day as computer technology advances, making it easier to steal data from computers. Understanding the problem of cybercrime is critical, as it has ramifications for our entire society. Customers have become reliant on digital payment systems as technology has advanced and the internet has become more accessible.[5] Checking bank balances, requesting bank statements and cheque books, upgrading debit cards, and even purchasing virtual products are among the

[3] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 265

[4] ibid

[5] ibid

options available. Financial organizations are increasingly utilizing social media channels to engage their clients in online payments.

Web technology has now become a vital as necessary aspect of the Indian Banking industry. The global expansion of non-cash transactions has resulted in the continual development of reliable online payment systems. While paper based transactions cleared through cheques totaled Rs. 85lac crore in FY15, paperless transaction totaled Rs. 92lacs crore, indulging retail electronic transaction such as ECS (Electronic Clearing System), debits and credits, electronic fund transfer, card transactions and prepaid instruments.[6] Due to greater online acceptance through alternative channels such as the internet, ATMs, and mobile banking, India has seen a growth in the volume of debit/credit cards. Cyber crime has increased dramatically in recent years across all industries and geographies. Organizations face a huge difficulty in being resistant to cyber-attacks, given the spread of these technical crimes. According to the National Crime Records Bureau's 2015 statistics on Motive-Based Cases Reported under Cyber Crimes, Greed / Financial Gain is the primary motivator for committing Cyber Crimes.

One of India's top private sector banks recently launched multi-social payment software, which allows consumers to send money via social media. Technology frauds accounted for 65 percent of the fraud instances recorded by banks, i.e. frauds conducted over or at an internet banking channel, ATMs, and other payment channels such as debit/credit/prepaid cards. Cyber scams are highly technical offenses. Cyber fraud is a difficult problem for law enforcement agencies to solve. To investigate cybercrime, law enforcement agencies must have qualified computer forensics personnel. [7]

According to statistics, India accounts for 7% of all cyber fraud incidents worldwide. Indian banks have been targeted by possible state and non-state actors, organized criminals, and hacktivists on a regular basis. The cyber-attack on Canara Bank in 2016 exemplifies this point, with a hacker from Pakistan attempting to disrupt the bank's e-payments by vandalizing its website and inserting dangerous software. [8]

---

[6] Rajan Sundaram, 'Rise of Cyber Crimes – How Are Banks Fighting Back?' (2020) <https://www.jigsawacademy.com/rise-of-cyber-crimes-how-are-banks-fighting-back/> accessed 10 June 2021

[7] ibid

[8] ibid

In July 2017, an attack on Union Bank of India's Nostro account resulted in the loss of over USD 170 million.

According to sources, the criminals used spear phishing to acquire access. According to a survey on cybercrime done by KPMG in 2017, banks were not initially adequately equipped with suitable cyber security mechanisms, as a result of which they were subjected to rampant cyber threats. The number of cases of cybercrime has risen from 89 percent to 94 percent, with financial losses rising from 45 percent to 63 percent. It also indicated that over 70% of respondents thought their organization was ill-equipped to combat cyber fraud. [9]

The inherent vulnerabilities in bank systems and software, the numerous entrance points to the internet, and obsolete defense technologies that are highly vulnerable to advanced attack technologies utilized by hackers are all major cyber security issues. The most basic goal of banking institutions, however, is mandated cyber security readiness. A variety of regulatory processes and cyber security technologies have been developed in recent years as a result of the growing dangers to the cyber infrastructure in its regulated businesses. As a result, given the growing frequency and complexity of cyber security incidents, a constant analysis of the cyber security landscape and emerging threats is required. The progress of banks in increasing their cyber security resilience and responsiveness will be tracked. [10]

1.2. STATEMENT OF THE PROBLEM

In present time, e-banking or online banking is used widely by majority of banks in most of the countries. It is also used in India for improved service and easier access to banking institutions. The use of e-banking is expanding, as are the challenges and crimes associated with it. Banks are the engines that drive the financial sectors operations that are critical to a country's economy. Thus, banks plays critical role in ay country's economic progress.

The number of cyber fraud in Indian banking industry rises in tandem with the growth of the banking sector's operation. Fraud in Indian banking is not a new occurrence. It is only allowed under the Information Technology Act of 2000, as

[9] ibid
[10] ibid

there are no clear and specific provisions relating to e-banking. E-banking security vulnerabilities are becoming more prevalent, posing challenges in providing services to the public. Unauthorized access to bank accounts by cyber criminals and other issues related to it are not receiving enough treatment."

1.3. AIMS AND OBJECTIVES

The main aim of this dissertation is to look into the laws and regulations governing e-banking or online banking in India as well as cyber frauds and its preventive and precautionary measures. This dissertation also aims at scrutinize the concerns related to cyber threat or cyber fraud in the banking industry by focusing on the underlying modus operandi. It emphasis on how well financial institutions are prepared to cop up with cyber crime situation. Therefore the objectives of this dissertation is summarized as follows –

1. To understand the development of E-banking in India.
2. To highlight the various securities issues relating to the E-banking in India.
3. To analyze the legislative framework that prevents cyber crime/ frauds in Indian Banking Industry.
4. To know the role played by Reserve Bank of India in E-banking.
5. To highlight the present scenario of cyber related crimes in Indian Banking Sector.

1.4. SCOPE AND LIMITATIONS

The purpose of this dissertation is to examine the breadth of e-banking and the scams that are associated with it in Indian banking industry. In this dissertation, the researcher looks at the concept of e-banking from an Indian legal standpoint. The study was limited to sorts of banking frauds, legislative framework, jurisdictional issues and the vigilance mechanism used by Indian banks by the researcher. Furthermore, the researcher will deal with reporting frauds to the Reserve Bank of India and a brief mention of the monitoring process within the vigilance system.

1.5. RESEARCH QUESTIONS

1. Why there is rise in cyber crimes in banking sector in India?
2. What is the present scenario of e-banking and its related cyber crimes in India?

3. Whether the Indian laws on cyber crime are adequate enough in curbing cyber crimes in Indian banking industry that posed to security issues?

1.6. RESEARCH METHODOLOGY

Research methodology involves the method through which research is conducted. The particular method used by the researcher is based on the collected and the available and the sources of data collection. The dissertation is based on the Legal Doctrinal the historical background of Indian banks and cyber fraud in Indian banking industry. The researcher has incorporated Doctrinal Methodology by using secondary sources which include books, journals, articles by prominent writers and internet sources. The researcher work is based on some secondary articles and journals of national as well as the international framework.

1.7. LITERATURE REVIEW

1. The book **"Information Technology Law (Cyber Laws)** by **Dr. S. R. Myneni** is based on Information Technology. In this book, the author has discussed elaborately about the meaning of E-Banking, its types, history, legal framework for E-Banking, advantage and disadvantage of E-banking, E-Banking in Indian context, E-banking in other countries, meaning cyber crime, history of cyber crime, classification of cyber crime, legal framework for cyber crime, detailed study of Information Technology Act, 2000, detailed study about phishing. This concept has been well explained in Chapter 3 of An Analytical Overview of E-Banking System in India and Chapter 4 of Cyber Crime in the Indian banking Industry.
2. The article **"A Critical Study on Concept of E Banking and Various Challenges of IT in India with Special Reference to RBI'S Role in Safe Banking Practices"** by **Jaro Jasmine & Ashwathy Ranjan** is based on E-banking system in India, RBI guidelines and IT laws that deals with e-banking system. In this article the author discussed about various E-banking services/products adopted by India, various challenges and issues faced by E-

Banking, advantages of e-banking to customers and bank and role of RBI to safe banking practices.

3. The article **"Electronic Banking in India: Innovations, Challenges and Opportunities"** by **Monisha & kanika Bhudhiraja** is based on electronic banking in India. In this article, they gave a brief idea about the concept of e-banking, its history, types, current scenario of internet banking in India, need and benefits of electronic banking, initiatives taken by the government of India for developing the internet banking, opportunities related to internet banking.
4. The article "**E-banking and Its Growth In India – A Synoptic View"** by **Suhash. D & H. N. Ramesh** is based on E-banking in Indian context. In this article the authors gave a conceptual view of E-banking, growth of e-banking in India, difference between traditional and electronic banking, electronic banking products in India, factors causing e-banking success and challenges in adopting e-banking.
5. The article **"Law Relating to E-Banking in India – An Outreach Challenge"** by **Dr. Suresh V. Nadagoundar & M. P. Chandrika** is based on legal provisions in e-banking in India. They have briefly discussed about the law relating to e-banking in India, obligations of the bank and the online banking, RBI circular to control risk due to internet banking. They also gave some valuable suggestions to curb e-banking fraud.
6. The article **"Challenges and Opportunities in E-banking in India** by **Sriram Devulapalli & Sai Karthik Oruganti** is based on e-banking in India. In this articles the authors has discussed about brief concept about e-banking, advantages of e-banking, opportunities related to e-banking, measures to be taken for safer e-banking.
7. The article **"A Study on Challenges and Opportunities in E-Banking sector in India"** by **K. Anitha** is based on e-banking industry in India. The author has discussed about various services provided by e-banking India, opportunities and challenges of e-banking in India.
8. The article **"Cyber-Crimes : A Growing Threat to Indian Banking Sector"** by **Simran & Akshay Manvikar & Vaishnavi Joshi & Jatin Guru** is based on cyber crimes in the Indian Banking Sector, financial fraud, fraud detection and identity theft. The authors has discussed about how advancement of technology has affected the banking industry. They gave an brief conceptual view on cyber

crime, how cyber crime operation works, preventive measures to control frauds. They have also discussed some case laws relating to cyber fraud in banking sector and they also suggested some precautionary measures to tackle cyber fraud in the Indian Banking sector.

9. The article **"Cyber Crime in Banking Sector"** by **Harshita Rao** is based on the cyber related frauds in the banking sector. The author has briefly discussed about different types of cyber fraud in this article, internet banking in India, how cyber crime is affecting the banking sector and its customers. In this article the author has also discussed some important and famous case laws on cyber crime in the Indian Banking Industry.
10. The article **"Information Technology and Cyber Law: A Globalized Review"** by **Mr. Rajib Bhattacharyya** is completely based on the growing emergence of information technology in the globe and the rising cyber space issues. In this article the author has given suffice conceptual view on cyber space and cyber fraud. The author has also scrutinized the IT legislation in India, objective of IT legislation and along with legislations of other countries that deals with cyber related crimes. In this article the author has explained the need for cyber law and the position of cyber law in India, history of cyber law in India, kinds of cyber crimes and preventive measures.

1.8. RESEARCH DESIGN

The research pattern of this dissertation includes the following structure:

- Chapter 1: Introduction
- Chapter 2: This chapter basically deals with an analytical overview on E-Banking system in India. It incorporates concept of E-banking, historical background of e-banking, various e-banking innovations that took place in India, features of e-banking, functions of e-banking, benefits and drawbacks of e-banking, opportunities and challenges of e-banking, present scenario of e-banking in India, initiatives taken by GOI for developing e-banking and conclusion.
- Chapter 3: This chapter basically deals with cyber crime in the Indian banking industry. This chapter incorporates conceptual view of cyber crime, historical background of cyber crime, techniques of cyber infringement in the banking

sector, impact of cyber fraud on bank's finance, cyber fraud safety mechanism in the banking sector, rise in cyber crime and reason behind it and growth in cyber crime during covid-19 pandemic.

- Chapter 4: This chapter primarily deals with cyber frauds in the banking industry- its legal and regulatory framework of cyber laws, historical background of cyber laws in India, need for cyber laws, Indian statutes and cyber fraud in Indian banking sector, role of RBI in e-banking and curbing cyber fraud, RBI circular to control risk due to e-banking, RBI guidelines and jurisdictional issues.
- Chapter 5: This chapter deals with judicial pronouncement on cyber fraud.
- Chapter 6: This chapter deals with conclusion and recommendation.

CHAPTER 2

AN ANALYTICAL OVERVIEW ON E-BANKING SYSTEM IN INDIA

2.1 CONCEPT OF E-BANKING

The world has become more dynamic and progressive as a result of science. It has resulted in changes in the economy, politics, culture, society, and individuals. This transformation is much more pronounced in the financial and banking industries. The financial sector plays a critical part in a country's economic development. An economy's lifeline is banking. For economic progress, a strong and healthy financial sector is essential. IT revolution is currently taking place in the banking sectors of India. The use of the internet in banking institutions has transformed the industry. Both customers and banks have profited from it. "Internet banking" or "e-banking" in India has seen a series of developments as a result of technological advancements and innovation. [11]

The word "e-banking" refers to a modem banking system. "E-banking" is a sort of banking service that uses an "electronic environment" (media) such as the 'Internet' to provide services to its customers. The entire procedure, in conjunction with "receiving or depositing money", "signature verification", "inventory", and other concerns, is done as an "Internet banking" activity in this sort of banking.

In the second part of the 1990s, "electronic banking" and the "World Wide Web (WWW)" prompted banks to employ electronic channels for obtaining instructions and render goods and services to clients. "E-banking" is a alternative method for users to access their "bank accounts", "pay bills", "manage their finances", and "take use of other banking related services". As a matter of fact, the utmost goal of establishing the "e-banking system" is to reduce and, if feasible, eliminate any references to the location of bank branches where financial services are provided. "E-banking" provides the customers of "banks" with convenient access to manage their monetary matters with the least amount of inconvenience possible, by providing a prompt and

[11] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 265

befitting way to perform different types of “banking transactions” through the “E-Banking website”, which is available 24/7 from home, office, or anywhere else. [12]

Electronic banking, virtual banking, online banking, and internet banking are all terms used to describe e-banking. Information technology-based banking is referred to as e-banking. A computer-controlled system is used to supply banking services because the computers ensured mathematical precision and promptness in banking. It has improved the speed, ease, and comfort of banking transactions. The client no longer has to carry a checkbook or cash money; instead, all he needs is a plastic card. However, the use of e-banking in our country is still quite limited. Thus, it is essentially the delivery of various financial products and services over an electronic and telecommunications network. A consumer can use his computer or mobile phone to access his account and conduct a variety of transactions using e-banking. In a way, it's similar to e-business in banking. . It enables customers of a financial institution to execute financial transactions on the firm's secure website, which might be a retail or virtual bank, credit union or building society.

E-Banking information architecture is modeled as client-server architecture. E-banking is the provision of online banking services to its customers over the internet using a personal computer (PC) or other internet-capable access device. Customers can use an “e-banking system” to manage accounts in both local and international currencies, as well as get all the information they need regarding the flow of funds on those accounts from anywhere in the world. A client using an Internet-connected PC accesses his bank's special “E-Banking site” and then logs in using a set of specific “secure numbers” to view and study their “bank accounts”, furthermore make any essential payments and make a transfer from his “personal bank accounts”. When the “transaction number” is used up, the “bank” provides them a new set of numbers for their separate “transfer sessions”. The “bank” may give “customized software” in particular circumstances. The “bank software program” can also be used offline, as for instance, to prepare payment orders “offline” before submitting them online. All numbers are sent to the client separately, primarily by mail. [13]

[12] ibid

[13] Monisha & Kanika Bhudhiraja, ‘Electronic banking in India: Innovations, Challenges and Opportunities (2017) 5 IJERT 1

Customers can use an e-banking system to manage accounts in both local and international currencies, as well as get all the information they need regarding the flow of funds on those accounts from anywhere in the world. To use an online banking facility provided by a financial institution, a "customer" with "personal internet" connection must "register" for the service and create a password (under several identities) for client verification.

In most cases, the "password" for "online banking" is different from the password for "telephone banking". However, consumers intend or not intend to use their "online banking facility", financial institutions now routinely assign client numbers (also known by other names). A single customer number might be linked to multiple accounts because "customer numbers" are not always the same as "account numbers". Any of the accounts that the client manages, such as checks, savings, loans, credit cards, and other accounts, will be linked to the customer number. Customer numbers will also differ from any debit or credit card provided to the customer by the banking institution. [14]

"E-banking" is defined in the legal language as "banking activities accessed by the use of a computer, modems, and telephones". In other terms, "E-Banking" refers to banking transactions conducted over the Internet. "The United Nations Conference on Trade and Development (UNCTAD)", on the other hand, provides a more complete and well-established definition. This term encompasses practically every aspect of electronic banking. [15]

2.2 HISTORY OF E-BANKING IN INDIA

As a consequence of the "E-Revolution", modern "banking" is more information-based, fast, and boundary-less. "E-banking", often known as "electronic funds transfer", is simply the use of "electronic means" to transfer funds from one account to another instead of using a check or cash. In 1981, the first version of what is now

[14] ibid

[15] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 265

known as internet banking was launched. New York City was the first city in the USA to try out a new way of doing business by offering "remote banking services". [16]

Due to the rising expansion of e-banking in India, it has gained general acceptance as a means of delivering financial services and as a strategic instrument for firm advancement. It is also swiftly catching up in India, with more and more banks entering the race. With the introduction of net banking, India appears to be on the verge of a massive banking revolution. In India, the Reserve Bank of India outlined its aim to ensure that payment and settlement systems are secure, effective, interoperable, approved, open, comprehensive, and compliant with international standards. The vision is to proactively energize the electronic payment framework in India in order to introduce a less trade society. [17]

Two consecutive Committees on Computerization (Rangarajan Committee) spawned the first initiative in the area of "bank computerization". The "first committee" was formed in 1984, and it drew out the "blueprint" for the banking industry's automation and computerization. The second Committee, established in 1989, prepared the path for the integrated use of telecommunications and computers in banking operations, allowing for full use of technology achievements. The focus switched from limited computerization using Advanced Ledger Posting Machines (ALPMs) to complete computerization at branches and branch integration. "Banks in India had 4776 ALPMs in branch offices, over 2000 programmers/systems personnel, and over 12000 Data Entry Terminal Operators until 1989."[18]

Until the 1990s, banks preferred conventional banking to branch banking. The banking industry evaluated the creative mobility of banking services after financial reforms. Since 1993, the Indian banking sector has welcomed computerization, more out of sheer necessity as well as compulsion to deal with rising overload and inconsistent of the manual system in order to assist additional expansion. In 1993, the "Indian Bank Employees' Association (IBA)" reached an "agreement" with "bank management" over the implementation of computerized applications in "banks". This

[16] ibid
[17] ibid
[18] Suhas. D & H. N. Ramesh, 'E-banking and it's Growth in India' (2018) 5 J Mgmt Res Analysis 376

"agreement" was a watershed moment in the use of computerized "applications" and the growth of bank "communication networks". However, the benchmark reports of two "committees" led by former "RBI governor Dr. C Rangarajan" sparked the first move in the domain of bank computerization. Both reports strongly advocated for the computerization of banking activities at all levels, as well as proper design. [19]

ICICI Bank was the first to implement E-banking in India in 1996. Following that, numerous other banks such as "HDFC, IndusInd, IDBI, Citibank Trust Banks, UTI", and others adopted the service. Because "private and foreign banks" have begun to capture the market through e-banking, "competition is heating up, and a lack of technology can cause a bank to lose a customer," public banks are breaking the shackles of traditional set-up and preparing to compete with their private sector counterparts. [20]

The usage of computer technology has a significant impact on the bank's operating patterns. The evolution of computerization in the banking industry can be clearly seen from 1966, when the first wage settlement with the bank union was signed addressing the use of ICT or IBM accounting machines for inter-branch reconciliation and other purposes. SBI began the process of installing a ledger-posting equipment with a mainframe computer at a few of its branches in 1970.

The Reserve Bank of India established a committee in 1994, led by W S Saraf that strongly advocated for the use of electronic funds transfer (EFT), the introduction of electronic clearing services, and the expansion of Magnetic Ink Character Recognition (MICR) beyond metropolitan cities and branches. By providing online banking services in its branches in 1996, the Industrial Credit and Investment Corporation of India became India's first to embrace electronic banking. HDFC Bank, IndusInd Bank, and Citibank were among the first to offer online banking services in 1999, following in its footsteps. The Reserve Bank of India and the Indian government have taken a number of steps to expand and improve the efficiency of electronic banking in

[19] ibid
[20] ibid

India. The Indian government passed the Information Technology Act of 2000, which gives e-transactions and e-commerce legal recognition. [21]

In the previous decade, foreign and private sector banks have dramatically increased their usage of information technology. The growing competition and global popularity of the internet phenomena are the key reasons behind this. The emergence of private and multinational banks with better technologically oriented financial services compelled Indian banks to adapt to technology advancements in order to remain competitive and retain customers. [22]

Beginning ATM and Point of Sale facilities in 1970, technology was a logical move for banks, which continued in the 1980s with the introduction of Tele- Banking and E- Banking in the 1990s. The Shared Payment Network System (SPNS) was introduced in February 1997, and it was a shared network of ATMs from 11 institutions. [23]

The ATM cards were given the brand name 'SWADHAN.' SPNS has the capability of connecting to worldwide hubs such as Master Card and VISA. CITI Bank offered the ATM card facility in India in 1985.

The following are some example of key technical advancements in India's new payment structures era:[24]

1. 1980-1990: Debit card and credit card have arrived.
2. 1984-1988: MICR cheques were introduced, and banks began to use computers.
3. 1987: HSBC launched the ATM concept in India for the first time.
4. 1990: RBI introduced the ECS payment was introduced in India.
5. 1991: India became a member of the Worldwide Interbank Financial Telecommunication society.
6. 1997: Shared payment network system was established.
7. 1999: RBI, IIT and IDBRT of Hyderabad collaborated on a smart card project.
8. 2000: Information Technology (IT) Act was passed.
9. 2002: Through SMS banking, the banks in India provided the facility of mobile banking to its customers.
10. 2003: Special Electronic Fund transfer was introduced.

[21] ibid
[22] ibid
[23] ibid
[24] ibid

11. 2004: RTGS was introduced.
12. 2005: Core banking solution had been implemented in 11% of public sector bank branches and national electronic fund transfer was introduced.
13. 2007: The Payment and Settlement System Act was passed.
14. 2008: Cheuqe truncation system was introduced and operative guidelines on mobile banking transactions were furnished.
15. 2009: Provision of free cash withdrawal from the ATMs was made.
16. 2010: Immediate payment service was introduced.
17. 2016: In August 2016, banks across the country began uploading their interfaces to the Bharat bill payment system and the Unified Payment Interface.
18. 2016: National Payments Corporation of India developed an app called BHIM (Bharat Interface for Money) based on UPI (Unified Payment Interface).[25]

Over the last ten years, significant developments have occurred, making banking clients' convenience the most crucial component of the business. The use of e-banking in India's major cities is well ahead of the rest of the country. Private networks, direct dial-up connections, public networks, and other new financial delivery mechanisms are available. ATMs, telephones, and personal computers are examples of banking devices. As a result of technology improvements, branch banking has given way to e-banking, sometimes known as "Anywhere Anytime Banking." Through the use of technology, banks were able to increase their operational efficiency.[26]

2.3 VARIOUS INNOVATIONS THAT TOOK PLACE IN E-BANKING

"Internet baking, Mobile Banking, Tele Banking, Debit Cards, Credit Cards, ATMs and Smart Cards" are all example of E-banking. Below the forms of E-banking are being explained –

- **Internet Banking –**

  The computerization of the financial sector has resulted in Internet Banking. As a consequence of the fierce rivalry, "banks" had no choice but to launch "internet

[25] ibid
[26] ibid

banking services". Furthermore, the fact that Internet banking is accessible at all times has given users a benefit. In the banking industry, there has been a paradigm change from "bricks and mortar" to "click and mortar." In 1999, ICICI Bank was the first bank to start "internet banking", followed by "IndusInd Bank and HDFC Bank". Internet banking is advantageous since it allows you to conduct "banking transactions" from the comfort of your own home or at your office workstation.
It is possible to avoid long lines and delays.[27]

Internet Banking can be accessed by simply logging in using a User ID and Password. A user can check his "account statement, transfer cash from one account to another, open an FD (fixed deposit), pay energy or telephone bills, pay rent, and recharge his or her postpaid or prepaid bills" with a single click on the internet. When using true internet banking, any query or transaction is performed online at any time, without the need to visit a branch (anywhere banking). As a result, delivering Internet banking is increasingly becoming a "must have" rather than a "good to have" service. [28]

Because it is the most cost-effective manner of providing banking services, net banking has become the standard rather than the exception in many developed countries. Online banking is feasible under this system, which provides each bank customer with a personal identification number (PIN) for performing online transactions with the bank via internet connections.[29]

The internet has created a level playing field, allowing customers open access to the global marketplace. For modernized financial institutions, internet banking provides a cost-effective delivery method. Consumers are enjoying many of the advantages of e-banking under this system. Having access to one's accounts via the World Wide Web (www) at any time and from any location is a convenient habit that was previously unknown. As a result, whenever a bank goes through a technology integration effort to enable its customer to access information about his or her personal account details, the bank's internet presence transforms from "brochure/ware" to "internet banking." [30]

[27] Monisha & Kanika Bhudhiraja, 'Electronic Banking in India: Innovations, Challenges and Opportunities (2017) 5 IJERT 1
[28] ibid
[29] ibid
[30] ibid

Certain security steps should be followed in order to keep one's bank account safe.

Personal information, such as PIN numbers and passwords, should never be shared with anybody, including bank workers. It is critical that documents containing confidential information are kept secure.

Before destroying the mailers, the PIN or password should be reset right away and memorized.

Customers should also refrain from sending important account information over insecure e-mail or over the phone. Simple safeguards like as changing ATM, PIN, and internet login and transaction passwords on a frequent basis are required. Along with these requirements, it is also necessary for the customer to make sure that the session which was logged in is logged out.[31]

Like every other things, internet banking also has its drawbacks. In India, there are some areas of worry when it comes to internet banking. In the meantime, a number of lawsuits involving fraud and deception of banks and clients have already been filed in India using this type of banking facility. Regardless, the RBI and banking authorities have attempted to promote the safety and soundness of online and e-banking facilities in the country by releasing essential guidelines. Member institutions ranked security as the most significant concern of online banking in a recent study conducted by the Online Banking Association. As a result, there is a twofold responsibility to protect clients' privacy as well as the product from fraud.

In present times, Internet banking has no alternatives. Indian banking is gradually getting more and more access of Internet banking. Thus, Internet banking would drive us into an age of creative destruction due to non-physical exchange; complete transparency is also giving rise to perfectly electronic market place and customer supremacy.

Following are the types of Internet Banking –

1. **National Electronic Fund Transfer (NEFT) :**

"National Electronic Fund Transfer (NEFT)" is a payment system which is accessible all over the country that encourages the transfer of balanced subsidizes. "People", "firms", and "corporations" can electronically transfer "assets" from any "bank" to

[31] ibid

any individual, firm, or corporation with a record at another participating bank office in the country. People, businesses, and corporations with bank accounts can use "NEFT" to transfer funds. Even those who do not have a bank account (stroll-in clients) can store money at "NEFT"-enabled branches with instructions on how to transfer funds via "NEFT". Such money settlements shall be limited to a maximum of "Rs.50,000" per exchange in any scenario. In this way, "NEFT" promotes originators and remitters to start subsidizing move exchanges even if they don't have any money. "NEFT" operates in hourly clumps; on weekdays (Monday through Friday), there are twelve settlements from "8 a.m. to 7 p.m.", and on Saturdays, there are six settlements from "8 a.m. to 1 p.m". [32]

2. **Real-Time Gross Settlement (RTGS) :**

"RTGS" is a method that allows "funds" to be moved in "real time" and on a "gross basis" from one bank to another. RTGS transactions can be carried out between banks or between clients using their bank accounts. "Real Time" refers to the "processing of instructions" as soon as they are received rather than later; "Gross Settlement" refers to the "individual settlement of funds transfer instructions (on an instruction by instruction basis)". The RTGS transactions are sort out one by one. [33]

RTGS transactions are processed by banks during normal business hours. Banks determine the hours of operation at their various branches based on their own conditions and rules. Customers can conduct RTGS transactions from "9:00 a.m. to 16:30 p.m". on weekdays and "9:00 a.m. to 14:00 p.m." on Saturdays, with settlement taking place at the RBI.

3. **Electronic Clearing System (ECS) :**

"ECS" is an optional strategy for impacting installment exchanges in regard to service charge installments, such as "phone charges, power charges, insurance premiums, card installments, and credit reimbursements, and so on" which would reduce the

[32] Suhas. D & H. N. Ramesh, 'E-banking and it's Growth in India' (2018) 5 J Mgmt Res Analysis 376

[33] ibid

need for banks/organizations/partners to give and manage paper instruments and, as a result, encourage improved client care. [34]

4. Immediate Payment Service :

IMPS provides interbank electronic store move management via cell phones in real time, 24 hours a day, seven days a week. IMPS is a deciding mechanism for moving money instantly within "banks" across "India" via "mobile, Internet, and ATM, which is not only secure but also efficient from both a monetary and non-monetary standpoint". [35]

- **Mobile Banking –**

The use of mobile phones to provide banking services has grown in importance. These days, we are completely reliant on our mobile phones. Due to the rapid growth of mobile phone subscribers in India, banking services are now available to customers via their mobile phones. Customers use their mobile phones to conduct transactions involving credit or debit to their accounts, which is known as mobile banking. The Reserve Bank of India (RBI) established a Mobile Banking Committee in 2014, which is chaired by B Sambamurthy. An investigation must be done by the committee on the challenges that has been experienced by banks in delivering mobile banking to their consumers, as well as the choices available, including the feasibility of employing encrypted SMS-based financial transfers.[36]

In our country, the use of mobile banking has increased dramatically. In terms of transaction volume, mobile wallets surpassed mobile banking in the 2016-2017 fiscal year. From April to November 2016, mobile wallet transactions trebled to around 400 million, ranging from phone recharges to paying for taxi or buying online.

Apps like Jugnoo, Ola, Uber, Mobikwik, Paytm, and others have mobile wallet systems. [37]

According to the Times of India, in the first eight months of the fiscal year 2016-2017, the number of mobile banking transactions more than doubled from 98 million to 265 million.

[34] ibid
[35] ibid
[36] ibid
[37] ibid

If the current rate of growth continues, it is apparent that mobile-based transactions, whether through a mobile wallet or a mobile banking transaction, will overtake the check payment system in a matter of months. [38]

In the current environment, mobile-based transactions totaled 602 million, accounting for 83 percent of the 723 million cheques processed from April to November 2015. However, until last year, the percentage of people who used mobile banking was less than 30%. In 2015, a client paid around Rs. 1.26 lakh crore using mobile payments, resulting in an 87 percent increase in mobile payment volumes.

- **Tele Banking :**

The second sort of e-banking innovation is telephone banking, which allows bank customers to do a variety of financial activities over the phone without having to visit a bank branch or an automated teller machine. Furthermore, telephone banking hours are substantially longer than branch hours, and some financial institutions even provide 24-hour service to their customers. [39]

Customers can conduct a variety of financial transactions using their telephone banking services, viz. –

a) Obtaining account balances
b) Lists of latest transactions
c) Electronic bill payments
d) Funds transfer between a customer's even in another's account

One of the most significant advantages of "telephone banking" is that it's reduces the necessity for "customers" to visit a "bank office" for "non-cash withdrawal and deposit transactions", lowering transaction processing costs.[40]

- **Automated Teller Machines (ATMs) –**

An ATM is a device which is located on or off the bank's premises. It enables a customer to withdraw cash, obtain statement of last few transactions in his/her account, deposit cash and to transfer funds from one account to another. A person can withdraw cash 24x7 from ATMs subject to the limit provided. This system is also

[38] ibid
[39] ibid
[40] Kavunthi Karunakaran, "Role of E-Banking in Current Scenario" (2019) 6 IJRAR 73

known as ‘Any Time Money’ or ‘Anywhere Money’. To have access of ATM a person must have an ATM card.[41]

After inserting the ATM card into the machine, the client must input a personal identification number (PIN). The PIN is a numeric password that is sent, handed over, or mailed to the consumer by the bank when the card is issued. After the initial usage, most banks require consumers to reset their PIN. Customers are also warned not to reveal their PIN to anybody, including bank personnel, by banks. Customers should change their PIN at least once a year. Transactions made with ATM machines are quite simple. [42]

External ATM and Interior ATM are the two types of ATM. External ATMs are those ATM which are found in shopping malls, train stations and airports, and interior ATMs are found within the banks facilities. The issuer bank sets the restrictions on cash withdrawals from ATMs and purchases of goods and services. A consumer can now withdraw cash from another bank's ATM as well. However, there is a cash withdrawal limit if the withdrawal is made at another bank's ATM. [43]

We can perform various financial transactions such as cash deposits, withdrawals, transfer funds, account information, ATM PIN change, and also linking the Aadhaar number to the bank account to reduce the interaction between the bank staff and the customer by using an automated teller machine or ATM.

India’s first ATM Card fraud - A group linked to digital malfeasance was nabbed by Chennai cops. Deepak Prem Manwani, a 22-year-old man who was discovered breaking into an “ATM” in “June”, was apprehended by the police. When he was apprehended, he had Rs 7.5 lakh in cash from two ATMs in “Chennai's” The “Nagar and Abiramipuram”, according to the police report. He had already taken “Rs 50,000” from an “ATM” in “Mumbai”.

“Manwani” was a Pune-based MBA dropout who was hired by a Chennai-based corporation. From a web bistro, he began his misdeeds. He had some European acquaintances who used to send him $5 credit cards from a handful of different

[41] ibid
[42] Ram Raj G, “Growth and Development of ATM in India” (2018) Asian Journal of Research in Bankin and Finance 64
[43] ibid

American banks. The administrator of the European site devised an intriguing strategy to obtain the clients' individual ID numbers.

That organization drew a sizable following. Evidently, Manwani and other supporters got into the arrangement of this pack and purchased a large amount of material on specified terms, and are essentially in an agreement on a decent sharing foundation. Manwani also learnt how to make 30 plastic cards with critical information on them, which he used to break into ATMs.

The FEI launched an inquiry after receiving numerous complaints from charged Visa clients and banks in the "United States", and alerted the "CBI" in "New Delhi" that a universal pack had evolved in "India" as well.

- **Smart Card –**

A "smart card" is a "pocket sized plastic card" with a computer chip installed in it. It also called "chip card" or an "integrated circuit card (ICC)". On one side of the card the "microprocessor" is hidden beneath a touch pad. Consider the microprocessor as replacement for the "magnetic stripe" on a "credit or debit card". The smart card "microprocessor" serves as a security feature. The microprocessor is spoken to by the host computer and card reader. Access to the data on the card is controlled by the microprocessor. These card "chips" are capable of a variety of "transactions, including cash withdrawal, deposits, and balance inquiry" among others. Below is the broad explanation of two forms of smart cards i.e. credit and debit cards: [44]

Debit cards are issued by banks and are linked to a customer's bank account. Debit cards can only be used to send money from one person to another within the United States. Currently, a consumer can use his Debit Card to withdraw money, obtain a monthly statement, and so on by visiting an ATM of a bank other than the one that issued the debit card. If a customer uses his debit card to make a transaction at an ATM of another bank from his savings account, his bank will not charge him for up to five transactions in a month, including both nonfinancial and financial transactions. [45]But in Delhi, Kolkata, Chennai, Mumbai and Benglore and Hyderabad, there are

[44] Monisha & Kanika Bhudhiraja, 'Electronic Banking in India: Innovations, Challenges and Opportunities (2017) 5 IJERT 1

[45] Jaro Jasmine & Aswathy Ranjan, "A Critical Study of Concept of E-banking and Various Challenges of IT in India with Special Referrance to RBI's Role in Safe Banking Practices" (2018) 119 IJPAM 1661

some limitations on the five free transactions made at another bank's ATM. These cities can make only three free transactions in other banks instead of five.
Credit cards are issued to customers by banks/other businesses approved by the RBI, just like debit cards. A credit card is a piece of plastic that symbolizes a credit line. It enables the cardholder to purchase goods and services on credit in exchange for a pledge to repay the money. [46]

A credit card is approximately "8.5 inches" long and wide. "5.5 cm x 5.5 cm". It's a little "rectangular plastic card" with the name of the cardholder, i.e. the customer, and the "account number" printed on top. Moreover, the card's validity period is stated. On the reverse, there will also be an embossed signature panel and a sample signature panel. A list of stores and businesses in each city where the card will be accepted in lieu of cash is also provided to cardholders and the upper limit which the cardholder can use to make purchases at a certain store. This restriction is also communicated to the cardholder every month. This is referred to as a card limit. [47]

Excessive use of credit cards has resulted from globalization and growing usage of the internet for online purchasing. It has a credit limit, which is a limit on how much money the owner can spend. At the end of the month, the owner has the option of paying the entire bill or a portion of it by the due date. It permits us to buy something expensive now and pay for it later. It is a particularly adaptable form of financing. [48]

It is true that something that has a lot of advantages also has some drawbacks. Credit card fraud is on the rise in today's world. While many of us have never been victims of credit card theft, it occurs on a daily basis. A transaction made with our account that we did not authorize is referred to as credit card fraud. It can be done when someone steals our credit card or our personal card credentials in order to conduct an unlawful transaction without our card being physically present. [49]

[46] ibid
[47] ibid
[48] ibid
[49] ibid

Some key differences between Credit and Debit Card:

Money is automatically taken out of our bank account when we use a debit card. In contrast, we pay the bill later when we use a credit card. If our bank account is empty, we can't use our debit card; nevertheless we can use our credit card even if our bank account is empty.[50]

A "debit card" is just a tool that can be used in lieu of cheque or cash. When we use a credit card, we are borrowing money. We use our funds when we use our debit cards. Whether we use credit or debit card, which is effectively cash, it entirely depends on how we want to spend and manage our money.

- **E-Cheque –**

One of the most recent inventions in e-banking is an e-cheque; it is a new type of payment mechanism that helps consumers who don't own a "credit or debit" card as a backup "payment method". Payment is made straight from the customer's bank account via the e-check technique. If a "customer's" "bank account" is the only payment option linked to their "bank account", they can only send an e-Cheque. You will not be able to send e-Cheques if the customer has a backup payment method.

2.4 FEATURES OF E-BANKING

I. Faster Transaction –

In this internet culture everything is fast. Customers that use e-banking have the ability to move money instantly because of the tremendous speed of internet. Customers save time because monies are transferred quickly from one account to another. E-banking is a fully automated system that operates over the internet. People no longer need to queue to transfer funds or pay their bills; they can do so quickly and conveniently using their mobile device. Customers save time because they can simply access their accounts using their mobile device.[51]

[50] Monisha & Kanika Bhudhiraja, 'Electronic Banking in India: Innovations, Challenges and Opportunities (2017) 5 IJERT 1

[51] Dr. Suresh V. Nadagoundar & M. P. Chandrika "Law Relating to E-banking in India – An Outreach Challenge" (2017) 2 ISSN 2321

II. Lowers Transaction Cost –

E-banking helps customers save money on financial transactions. Electronic transactions are referred to as the most cost-effective method of conducting business. As the workload has decreased, manpower requirements have decreased. The entire transaction takes place over the internet. Because all transactions are documented digitally, it has also decreased paperwork in organizations. Each record does not need to be manually entered and stored. [52]

III. Provides 24*7 service –

24*7 service is the most significant feature of E-banking. Customers can access their accounts at any time and from anywhere. It benefits clients by allowing them to do transactions according to their preferences.[53]

IV. Reduces the chance of error –

Human error has been decreased due to e-banking. It has diminished the function of the human in the transaction process as a whole. E-banking is a fully automated online banking system. All transactions are digitally recorded and preserved. There is no need to keep track of each and every record in the books of account by hand. As a result, the odds of human error are reduced. [54]

V. Develops loyalty in customers –

E-banking aids banks in attracting a huge number of committed consumers. Banks are able to provide excellent service to their consumers by using E-banking services. They are able to serve clients with faster and better service. The banking website provides customers with a user-friendly layout. They can access services at any time, even from the comfort of their own homes. When clients are cotented with the services provided by their "banks", they build a sense of loyalty. [55]

[52] ibid
[53] ibid
[54] ibid
[55] Divya. K, "Legal Aspects of Internet Banking in India" (2019) 2 IJLMH 1

VI. Removes geographical barriers –

E-banking has eliminated all transactional barriers due to distance. It has eliminated all distance constraints that clients previously faced when transacting in the traditional manner. E-banking allows for both domestic and international fund transfers in real time. All of the systems are online connected, allowing for quick money transfers. [56]

VII. Provides better productivity –

It plays an important role in enhancing corporate productivity. Automated software systems underpin the whole financial transaction system. These systems are specifically intended to handle financial transactions. It minimizes the amount of time it takes to complete transactions and the amount of labor that corporate organizations have to accomplish. They don't need to store anything manually because everything is stored digitally. It improves the firms' overall productivity. [57]

VIII. Reduce frauds in transactions –

Another useful characteristic of e-banking is that it allows for continual account monitoring. You can effortlessly keep track of all of your accounts' transactions. If somebody commits fraud in financial transactions, you can easily track it down. It creates a complete digital trace of everyone who has access to your banking information and can commit fraud. As a result, your accounts become more transparent, lowering the risk of fraud. [58]

2.4.1 FUNCTIONS OF E-BANKING

The following services are provided by e-banking system by the banks to its customers for easy banking experience –

1. **Pay a bill –**

   Every bank has a tie-up with different utility companies, service providers, insurance companies, etc. across the country. The banks use these tie-ups to offer online payment of bills (electricity, telephone, mobile phone, etc.). Also, most banks charge a nominal one-time registration fee for this service.

[56] Jaro Jasmine & Aswathy Ranjan, "A Critical Study of Concept of E-banking and Various Challenges of IT in India with Special Referrance to RBI's Role in Safe Banking Practices" (2018) 119 IJPAM 1661
[57] ibid
[58] Rachit Garg, 'Legal Issues in Internet Banking' (2020) < https://blog.ipleaders.in/legal-issues-internet-banking/ > accessed 20 June, 2021

Further, the customer can create a standing instruction to pay recurring bills automatically every month.[59]

A depositor can use an electronic bill payment service to send money from his or her online account to a creditor or merchant, such as a public utility or a store. You don't have to wait in a large line on a Sunday morning to complete your transactions! The payment is almost instantaneous, though certain banking institutions may choose to transmit the payment the next business day. The bank can print and mail a paper cheque or banker's draft to a creditor who is not set up to receive electronic payments if necessary.[60]

2. **Schedule payment in advance –**

The option to plan a payment on a specific date is recommended by most institutions. The money is automatically withdrawn from our online bank account once the amount is input and the payee is checked. It's especially handy if we have a habit of forgetting deadlines. We can, for example, plan credit card or mortgage payments to avoid incurring late fees and damaging your FICO score.[61]

3. **Inquire about information of account –**

The client requests information about his own account, such as the card's / account's balance and the account's full historical records, and downloads the report list.[62]

4. **Transfer funds –**

Anywhere in India, a consumer can transfer funds from one account to another with the same bank or even a different bank. He must log into his account and provide the payee's name, account number, bank, and branch, as well as the amount to be sent. The transfer takes around a day to complete. [63]

[59] Nilutpal Deb Roy, 'E-banking Frauds and Indian Legal Prospective' (2020) <http://www.legalserviceindia.com/legal/all_aricles-6595-nilutpal1551.html > accessed 21 June, 2021
[60] ibid
[61] ibid
[62] ibid
[63] ibid

5. **Investing –**

   A consumer can open a fixed deposit with the bank online by cash transfer using electronic banking. A consumer can also purchase or sell shares online if he has a demat account, a linked bank account, and a trading account. Furthermore, some banks allow users to buy and sell mutual fund units through their online platforms.[64]

6. **Bank securities account transfer –**

   Through e-banking now the client can move funds between his own bank savings accounts, his own Credit Card account, and his own securities business capital account. Furthermore, the client has the ability to query about the current balance in real time.[65]

7. **Foreign exchange transaction –**

   When the client shops on the designated website, he or she can make a real-time transfer and receive payment confirmation from our bank. [66]

8. **Client service –**

   The client can modify the login password, information of the Credit Card and the client information in e-bank on net.[67]

9. **Account management –**

   The client can change his own account's rights and status in the personal e-bank, such as changing his login password, freezing or deleting specific cards, and so on.[68]

10. **Reporting the loss if any –**

    When a client's credit card or passbook is lost or stolen, the client can report the loss locally (not nationally).[69]

---

[64] Nilutpal Deb Roy, 'E-banking Frauds and Indian Legal Prospective' (2020) <http://www.legalserviceindia.com/legal/all_aricles-6595-nilutpal1551.html > accessed 21 June, 2021

[65] ibid

[66] ibid

[67] ibid

[68] ibid

[69] ibid

11. Shopping –

With an e-banking service, a customer can purchase goods or services online and also pay for them using his account. Now shopping is at our fingertips.

12. Cashless Transaction –

Another important function of e-banking is cashless transaction. After the emergence of e-banking, the burden of carry cash has been reduced. Now payments can be done electronically through internet banking instantly.

13. Apply for a loan or credit cards–

We can apply for a credit card or a loan (auto loan, student loan, mortgage, home equity loan, etc.) from the same bank by utilizing an online account. The application is more likely to be accepted if we have an excellent credit score and a lengthy relationship with our bank.

14. Order a cheque book –

Ordering a check book online allows us to save time. When we receive notification that our check book is available for pickup, we will need to visit our bank once.

15. Track payment history –

We can search for payments using online banking by transaction type, date, description, or amount. When was the last time we paid Company X? What year did we purchase your computer? To whom did we most recently make a payment? Our bank has all of the answers.

16. Chat with customer assistant department –

If we require assistance, we can contact our bank's customer service department. They will contact us and make every effort to resolve our issue.

17. Get alerts –

This service allows us to receive timely e-mail updates from our bank regarding any significant changes to our Internet accounts. We can, for

example, receive notifications when we make a withdrawal or modify our contact information.

18. **View up-to-the-minute account statements and balance –**

    To check account balances, you don't have to wait for your bank statement to arrive at your P.O.Box. By going into our online account every day, we can see all of our transactions and withdrawals. We can also report any inaccuracies or unlawful transactions in our statement right away.

19. **Manage all accounts in one place –**

    Online banking saves time by allowing you to manage multiple bank accounts (checking, savings, CDs, IRAs, and so on) from a single location. The majority of new accounts you create will be added to OB automatically (Online Banking).

20. **Take advantage of online brokerage –**

    We can invest via internet banking. Trades can be made and confirmed at any time, seven days a week. Most banks provide a diverse selection of money market products from a variety of issuers.

2.4.2 BENEFITS AND DRAWBACKS OF E-BANKING

In the previous three decades, banking has seen several advances, one of the most notable of which is e-banking, which is the product of the information and technological revolution. These IT revolutions transformed the banking sector's overall operation, as e-banking spawned a new class of financial services based on the convergence of traditional retail financial services and the internet. E-banking is the provision of basic banking services or transactions via the internet.

Due to the implementation of E-banking system, the banking system has grown more valuable, easier to use and saves time. Now we can pay bills, transfer funds, and view account statements from the comfort of our own homes, which was previously unavailable. However, some of these valuable services come with benefits and drawbacks. The following are some of the advantages and disadvantages of using an electronic banking system.

- **Advantages of E-banking:**

a) Convenience –

This is one of among most essential benefit of "internet banking" that outweighs any disadvantages. Making transactions and payments at the touch of a button without having to leave the house or workplace is a convenience that no one wants to give up. When compared to visiting to the bank, keeping track of accounts by using "internet" is faster and more suitable. Non-transactional services such as obtaining check books online, updating accounts, enquiring about interest rates for various financial products etc. become easier to do on the internet. [70]

b) Time saving –

With the introduction of e-banking, banking has become much more convenient and time-saving.E-banking main goal is to give customers with convenient and safe ways to do online financial activities such as automatic deposits, automatic bill payments from their bank account, and online loan applications, among other things.[71]

c) Simple and transparent process –

Customers contact their bank and then enter their user id and password on their bank's Web site to gain full access to their account, which is a very easy and transparent process. All they require is a secure Web browser. This method of online banking demands the use of Internet browsers that enable 128-bit encryption, which protects customers by encrypting all personal data sent between their computer and the bank. This, in turn, leads to increased consumer satisfaction.[72]

d) New innovations in banking sector –

Latest product design, numerous means of conducting "online financial transactions" and various "electronic systems" have all resulted from the introduction of innovation in the "banking sector". All of this gave rise to the term "innovative banking," which has become a common moniker for today's banking sector. The focus of innovation

[70] Sriram Devulapalli & Sai Karthik Oruganti, "Challenges and Opportunities in E-Banking in India" (2019) 5 IOSR – JBM 56
[71] ibid
[72] ibid

banking is mostly on consumer ease and satisfaction.[73] The primary motivation for introducing innovation into the "current banking system" was to provide customers with improved services via the use of technology, and the internet served as the foundation stone for innovation banking in this race of technological growth. Because of the replacement of paper-based and labor-intensive methods with automated processes, drastic changes such as higher efficiency, control of operations, and cost reduction were observed after the introduction of the internet in the banking sector. This resulted in higher productivity and profitability. [74]The need for innovations in the financial sector was recognized as a result of many obstacles that existed in the conventional banking system; however, these challenges were addressed after the introduction of innovative banking products and services, which completely revolutionized the banking mindset.

e) Bette Rates –

Banks stand to benefit greatly from the adoption of internet banking because it requires less physical effort on their part. The need for larger office facilities and more people to deal with customers is greatly reduced, resulting in huge financial savings for banks. This means that a portion of the savings can be passed on to consumers in the form of higher deposit rates and lower lending rates. To encourage internet banking, most banks provide no-deposit or low-deposit accounts, as well as reduced penalties for early withdrawal of Fixed Deposits.[75]

f) Services –

By just signing in, technology has made it exceedingly convenient for both the bank and the consumer to access a variety of excellent services. Financial planning capabilities, functional budgeting and forecasting tools, loan calculators, investment research tools, and stock trading platforms are among the services available on the bank's website as easy applications. Additionally, most banks offer online tax forms and tax preparation services.[76]

[73] ibid
[74] ibid
[75] ibid
[76] ibid

g) Mobility –

In recent years, internet banking has progressed a lot in the form of mobile internet banking, which provides customers with unlimited mobility and allows them to conduct financial transactions while on the go.[77]

h) Environment friendly –

Another significant advantage of online banking is that it is good for the environment, as it decreases paper usage, pollution, and emissions by eliminating the need for individuals to travel physically. However, the present trend of primarily using the internet mode to conduct all types of transactions has a few hazards that, if not avoided from the start, could be costly in the long term.

- **Disadvantages of E-Banking:**

a) Relationship –

The conventional visit to the branch office used to create a relationship with the banker, but online transactions have taken a toll on that relationship. When requesting a faster loan approval or a specific service that is not available to the general public, having a personal relationship with bank staff comes in helpful. The manager has several discretionary abilities, such as waiving penal interest or service fees, which are frequently used by employees who have a superior understanding of the company. Furthermore, having a personal relationship with a banker meant that the banker could provide valuable financial advice and insights to the customer.[78]

b) Complex Transaction –

Many difficult transactions cannot be resolved without a face-to-face conversation with the manager, which is not possible with internet banking. Specific problems and complaints require a personal visit to the bank, which cannot be accomplished via the internet. Many sophisticated service issues are difficult to resolve because online

[77] Sriram Devulapalli & Sai Karthik Oruganti, "Challenges and Opportunities in E-Banking in India" (2019) 5 IOSR – JBM 56

[78] K. Anitha, "A Study on Challenges and Opportunities I E-Banking Sector in India" (2019) 7 Shanlax Int'l J Comm 14

communication is neither clear nor precise.[79]Notarization and bank signature guarantee are two services that cannot be completed online.

c) Security –

This is the most serious flaw in the internet banking method, which the average user must avoid. Despite the fact that your account is protected by a slew of sophisticated encryption software, there is always the possibility of cyber-hacking by astute cyber-criminals. On the internet, "hacker attacks", "phishing", "malware", and other forms of unwanted activity are all too frequent. Identity theft is another major risk for those who rely only on the internet for their banking. To combat identity theft, most banks have made it essential to post scanned copies of approved checks online.[80]

d) The trust factor –

For most customers, the largest barrier to internet banking is trust. Customers choose traditional banking over internet banking due to a lack of trust in online security. They believe that internet transactions are hazardous and that fraud can occur as a result. Customers have a variety of questions when utilizing e-banking services, such as: Did the transaction go through? Is it true that I pressed the transfer button once or twice? One of the most important variables that influence a customer's willingness to transact with a web merchant is trust. [81]

e) Customer awareness –

In India, consumer awareness of "e-banking" facilities and procedures is still low. "Banks" are unable to convey accurate information regarding online banking use, benefits, and features. One of the most cited barriers to the development of "e-banking" is a lack of awareness of new technology and their benefits.[82]

[79] ibid
[80] ibid
[81] ibid
[82] ibid

2.4.3 OPPORTUNITIES AND CHALLENGES OF E-BANKING:

Opportunities in E-Banking

- **Various channels -**

  To grow banking business, banks can provide a variety of ways for customers to access their banking and other services, such as ATMs, local branches, "telephone/mobile banking", video banking, and so on. [83]

- **Bill payment services** –

  Because each bank has tie-ups with various utility companies, service providers, and insurance companies across the country, e-banking can help with the payment of power and telephone bills, as well as mobile phone, credit card, and insurance premium bills. It is important to increasing the number of people who use the internet and their computer literacy. It is a very necessary or initial prerequisite to use internet banking that people understand internet technology so that they can readily embrace internet banking services. [84]The rapidly growing number of internet users in India represents a significant opportunity for the banking industry, which should seize this opportunity to encourage more internet users to use internet banking services.

- **Creating high value digital services to customers –**

  Over the last decade, customer behavior and expectations have shifted dramatically. The shift to digital is evident across the board, with the financial industry leading the way. Customers can use their preferred channel to access banking services at any time and from anywhere. Customers can do simple banking transactions using a smart phone, PC, or laptop while sitting at their desk or at home.[85] Customers can request drafts by e-mail and have them delivered to their doorstep. As a result, E-banking makes home banking easier.

[83] Kumari Nidhi, "E-Bnaking in India: Challenges and Opportunities" (2016) 5 Int'l J Sci Mgmt 809
[84] ibid
[85] ibid

- **Competitive advantage** –

  The advantage of using e-banking gives banks a competitive advantage over other players. The use of e-banking is helpful to the bank in a number of ways, including cost savings, improved customer relations, and expanded geographic reach. The advantage of e-banking is that it allows banks to better manage their banking operations.[86]

- **Capability** –

  By providing Internet connectivity to their consumers, banks can become even more efficient than they are now. The bank benefits from an almost paperless operation thanks to the Internet. E-banking provides a solid foundation for banks to provide a variety of cash management products and branch out into new areas such as e-commerce and EDI.[87]

- **Escalating the number of internet users and computer literacy** –

  To use online banking, it is essential or a pre-requisite that consumers have a basic understanding of internet technology so that they may quickly embrace the services. The rapidly growing number of internet users in India represents a significant opportunity for the banking industry, which should seize this opportunity to encourage more internet users to use internet banking services.[88]

- **Initiative taken by Government Agencies for financial literacy**–

  "In order to achieve financial inclusion and inclusive growth, financial literacy and education are essential. According to a study, financial literacy has a significant impact on internet banking use. If customers are not financially educated, they will simply avoid using new online services and will not change their traditional banking habits, preventing banks from converting users to their new online banking strategies. Various government entities, such as the RBI, SEBI, IRDA, and other market participants, have taken a variety of financial education programs. [89]They have developed a school curriculum that covers a variety of topics such as online banking,

[86] ibid
[87] ibid
[88] ibid
[89] ibid

banking products and services, and net banking in order to teach school kids, college students, working executives, middle-income groups, homemakers, retired personnel, and self-help groups."

- **Worthy customer service –**

  Customer service that is worthy of a bank's brand is the ideal brand ambassador for expanding the bank's business. Every interaction with a customer is an opportunity to build trust in the bank. Customer service has become the backbone for measuring a bank's success in the face of increased competition. [90]

- **Retail lending –**

  Banks have recently used client segmentation, which has greatly aided in the customization of their product portfolios. As a result, retail lending has become a focal area, particularly in the financing of consumer durables, houses, autos, and other such items. Retail lending has also aided in risk dispersal and improved bank revenues through higher recovery rates. [91]

- **Untapped rural market –**

  The banking business in India has a largely unexplored market, accounting for 70% of the entire population. Banking services are now available in all urban areas, but only a few large villages have banks. Because the bulk of Indians still live in rural regions, the banks must reach all remaining communities. [92]

Challenges of E-Banking

- **Security issues** –

  Security concerns and other associated challenges have become a top priority for the banking industry. Because of safety and security concerns, a large percentage of clients are hesitant to use e-banking services. According to the IAMAI Report (2006), 43 percent of internet users in India still refuse to use internet banking due to security

[90] Kumari Nidhi, "E-Bnaking in India: Challenges and Opportunities" (2016) 5 Int'l J Sci Mgmt 809
[91] ibid
[92] ibid

concerns. As a result, banks face a major task in persuading customers of this benefit, which might boost online banking usage even further. [93]

- **Trust issues** –

  For most customers, trust is the most significant barrier to electronic banking. Customers frequently prefer traditional banking due to their lack of trust in internet banking transactions. They believe there is a risk in online banking transactions, which can lead to various frauds and scams. Consumers who use online banking services always have a doubt or a question in their minds about whether or not the transaction will be completed successfully until they receive a confirmation message.

- **Supervisory and operational issues –**

  The risk of direct or indirect loss coming from insufficient or failed internal processes, people, and systems, as well as external events, is known as operational risk. They are also known as Transactional Risks and are the most common risk connected with internet banking. Operational hazards include inaccuracies in transaction processing, contract non-enforceability, unauthorized access, and penetration into the bank's system, among others. This type of risk is usually caused by poor banking software design, other technological inefficiencies, human negligence, employee fraud, and so on. Although there is a fine border between security and operational challenges, they are frequently used interchangeably.

- **Authentication issues –**

  To confirm the authenticity of an instrument, security processes such as PIN numbers, Customer Relationship Numbers, Passwords, OTPs, Account Numbers, and so on are used. Different countries have established different criteria for determining the validity of a transaction. The Information Technology Act of 2000 in India stipulates that any subscriber may use a Digital Signature to authenticate his electronic record. The problem with authentication is that the Act only acknowledges one type of technology for authenticating electronic documents (the asymmetric cryptosystem), which creates questions about whether the legislation recognizes other financial authentication methods.

[93] Dr. Prof. Renu & Kuldeep Singh, "The Impact of E-Banking on the use of E-Services & Customers Satisfaction" (2019) 3 IJTSRD 20

- **Risk of privacy** –

  One of the key reasons that consumers are hesitant to use electronic banking services is the risk of revealing non-public or personal information, as well as the fear of identity theft. A huge number of consumers fear that by using internet banking services, their identity may be jeopardized. Consumers are concerned about their privacy since banks may intrude on their privacy by utilizing their information for marketing and other consequential purposes without their consent, according to the research.[94]

- **Extortion of funds –**

  Due to client privacy violations, there is a risk of personal data leakage, stolen card data, and illegal data sharing in banks. Cyber-attacks have taken on new forms as a result of technological advancements, such as web attacks and ransomware. In general, cyber-attacks on banks include the extortion of funds from individuals to organizations. Phishing emails are used to steal confidential credentials, and monies are syphoned through whaling. It is difficult for banks and financial institutions to manage threats from many cyber-attacks, as customers expect banks to guarantee data security. The main issue is that bank employees and customers are unaware of cyber dangers and their devastating consequences. In India, banks are also finding it challenging to manage and comply to regulatory compliance, since the number of regulations has expanded in recent years.[95]

- **Customer awareness** –

  In the Indian context, consumer knowledge or awareness of e-banking is still on the low side. Banks are unable to publicize all aspects of online banking, including its use, benefits, and features. As a result, one of the most significant roadblocks to the expansion of electronic banking is clients' lack of awareness of new technologies.[96]

[94] ibid
[95] ibid
[96] ibid

- **Less dissemination of internet in India** –

  Over time, the internet banking channel has evolved. In India, e-banking adoption increased from 1% in 2006 to 7% in 2011, whereas in North America, 60 percent of important bank transactions were completed through internet channels in 2011. (Infosys Report, 2012). As a result, it can be stated that knowledge and availability of the internet is still one of the most pressing issues in the Indian setting. According to an IAMAI 2006 research, approximately 22% of internet users are unaware of how to transfer payments online. As a result, the penetration of internet customers and online knowledge are the key challenges.[97]

- **Operating conditions** –

  India is a country with many cultures and languages, yet this complicates the online banking operating methodology because showing instructions or guidelines in different languages is a time-consuming operation. Nonetheless, technology has found a solution to this problem; however, illiterate people are still excluded from this solution, and ATMs cannot ensure similar functioning levels from all users, resulting in excessive wear and tear.[98]

- **Technological illiteracy** –

  Many lower-class mobile users do not comprehend the technical laws and regulations that govern mobile banking, and as a result, they find it difficult to utilize. Consumers typically purchase handsets based on their budget, and these handsets may have capabilities that are incompatible with Mobile Banking, posing a barrier to e-banking execution.[99]

- **Training the employees** –

  Training bank employees is a simpler process in private sector banks since they have young, energetic computer savvy people, whereas training employees in public sector banks is a more difficult task because the current staff is significantly less computer

[97] Dr. Prof. Renu & Kuldeep Singh, "The Impact of E-Banking on the use of E-Services & Customers Satisfaction" (2019) 3 IJTSRD 20

[98] ibid

[99] ibid

educated. Despite this, they have been able to have a significant impact after working on it for over a decade.

- **Customer education** –

  In the case of private banks, consumers have had access to e-banking services since the beginning. However, it is difficult to persuade clients of the benefit of this program in the case of ancient public sector banks. It is difficult to provide formal e-banking education to customers.[100]

  In light of this, banks have begun to offer monetary incentives to customers, such as a free debit card, free Net Banking services, and constant and timely information about monthly statements of their accounts via email, among other things, in order to encourage them to use these growing banking services.

- **Restricted business**–

  Another issue with e-banking is that not all financial transactions can be completed online or through other electronic means; for some services, such as deposits and withdrawals, one must visit a bank in person. Although it has been observed that some banks have automated their methods and customers (front end), many continue to use the old way (back end)[101]. Due to a lack of information and technical challenges, this effectively limits clients.

- **Non-Performing Assets (NPA)**–

  Nonperforming assets (NPAs) are another issue facing the banking industry. Due to rising interest rates, constraints on collection techniques, and skyrocketing real estate prices, vehicle loans and unsecured loans increased N.P.A., accounting for 50 percent of the bank's retail portfolio. As a result, every bank must ensure that loans are paid back on time.[102]

- **Competition**–

  Foreign and new private sector banks are putting pressure on nationalized and commercial banks. In the banking industry, banks face a variety of issues, including product positioning, innovative ideas and channels, new market trends, cross-selling,

[100] ibid
[101] ibid
[102] ibid

and managing assets and risk. Banks are limiting their administrative folio by converting human to machine power, i.e., banks are reducing physical labor and maximizing the use of machine power. The use of skilled and specialized manpower will be made, and result-oriented, focused personnel will be appointed.

2.5 PRESENT SCENARIO OF E-BANKING IN INDIA

E-banking practices in India are substantially lower than in Western countries. Banks have worked to build information infrastructure to improve E-banking operations in recent years. However, in India E-banking has become an important aspect of the banking system. Traditional banking, i.e. branch-based banking, was prominent until the early 1990s, when non-branch financial services were introduced. ICICI Bank is responsible for the introduction of internet banking in India. In 1999, Citibank and HDFC Bank launched internet banking services. With effect from October 17, 2000, the Government of India enacted the IT Act, 2000, which gave legal legitimacy to electronic transactions and other forms of electronic business.[103]

To deal with the pressures of increased competition, Indian commercial banks have implemented a number of initiatives, one of which is e-banking. The competition has been particularly fierce for public sector banks, as newly founded private sector and foreign institutions have been pioneers in e-banking adoption. [104]

Commercial banks in India have taken many steps to improve banking services and acquire a competitive advantage in the face of increasing competition.[105] The following are a few of the e-banking initiatives taken by Indian banks:

- Recently, the bank of India has announced the availability of card-less cash withdrawal service to its customers.
- The Bank of Baroda has implemented the Business Transformation Program, which will offer its customers comfort banking 24*7 in India and overseas using integrated delivery channels such as the Internet, phone, mobile, and others. [106]

[103] A. R. Raghaban & Latha Parthiban, "The Effect of Cyber Crime on A Bank's Finance" (2014) 2 Int'l J current Res Ac Rev 173
[104] Kavunthi Karunakaran, "Role of E-Banking in Current Scenario" (2019) 6 IJRAR 73
[105] ibid
[106] ibid

- On behalf of the Central Board of Direct Taxes, GOI, a number of Indian banks have deployed the Online Tax Accounting System (OLTAS). [107]
- ICICI Bank has introduced electronic branches that are open 24 hours a day, seven days a week and are a one-stop shop for all banking transactions. It provides services such as a check deposit machine and an electronic kiosk where consumers can access online banking. E-Locker is a service offered by ICICI Bank to its customers. It is a virtual locker that customers may access through ICICI internet banking to store soft copies of key papers such as legal documents, agreements, policies, and various important certificates in a secure manner. Customers who use internet banking for the first time will receive a variety of rewards from ICICI Bank.
- Banks are using social media platforms such as Facebook and Twitter to reach out to a large client base as well as new consumers; there will be round-the-clock tweets and comments on the bank's products and services. SBI expanded its social media presence by opening a Twitter handle, following the introduction of accounts on Facebook and YouTube.

Although Indian banks are making genuine attempts to adopt modern technology and set up e-delivery channels, the concept and scope of E-banking are still evolving. It provides an efficient payment and accounting system, resulting in a significant increase in the speed with which banking services are delivered. While e-banking has improved efficiency and convenience, it has also presented regulators and supervisors with a number of issues. The development of E-banking in India has been aided by several measures taken by the Indian government and the Reserve Bank of India (RBI). As previously stated, the Indian government passed the Information Technology Act of 2000, which gives legal status to electronic transactions and other forms of electronic business.[108] The Reserve Bank of India has been working on upgrading its role as a regulator and supervisor of the technologically driven financial sector. It issued risk and control guidelines for computer and telecommunication systems to all banks, recommending them to assess the inherent hazards in the systems and implement suitable control mechanisms to handle these risks.

[107] ibid

[108] Kavunthi Karunakaran, "Role of E-Banking in Current Scenario" (2019) 6 IJRAR 73

E-banking is now governed by the same regulatory framework that governs banks. It covers a wide range of topics related to technology, security standards, and legal and regulatory challenges.

2.6 INITIATIVES TAKEN BY GOI FOR DEVELOPING E-BANKING

With the objective of promotion and encouragement of the applications of E-Banking, various initiatives have been taken by RBI and Indian Government.

- The Government of India (GOI) passed the IT Act 2000 on October 17, 2000, with the goal of legalizing electronic transactions and other forms of electronic commerce.[109]
- RBI conducts ongoing review of E-Banking legislation requirements to ensure that the nation's financial stability is not jeopardized by E-Banking challenges.[110]
- The Dr. K.C. Chakrabarty Committee, which included members from IIM, IDRBT, IIT, and the Reserve Bank of India, framed the Vision Document 2011-17, which presents an analytical road map, i.e. strategy, to enhance the relevance of IT in the banking sector [RBI (2011), "IT Vision of Reserve Bank of India 2011-2017"].
- Attempts to Improve the Security of the Payment SysteBy the RBI. As a result, banks have been encouraged to strengthen their e-banking security features. The Reserve Bank of India has stated that using alternative payment channels such as mobile banking and ATMs places an additional obligation on banks to ensure safe and secure transactions. (Source: RBI Annual Report) (2013).[111]
- The Reserve Bank of India (RBI) has given the National Payments Corporation of India (NPCI) permission to expand mobile banking services and IMPS (Immediate Payment Service) channels such as ATMs, the internet, and mobile phones. Aside from that, NPCI is working to bring in more mobile network providers so that mobile banking services can be made available

[109] Sriram Devulapalli & Sai Karthik Oruganti, "Challenges and Opportunities in E-Banking in India" (2019) 5 IOSR – JBM 56

[110] ibid

[111] ibid

through a single platform. (From the 2013 Annual Report of the Reserve Bank of India.)[112]

- Risk management guidelines for electronic banking have been highlighted by the Basel Committee on Banking Supervision (2001).They focus on adapting and extending the existing risk-management strategy to the electronic banking structure.[113]

2.7CONCLUSION

The next generation of electronic banking transactions, E-Banking has opened up a new window of opportunity for existing banks and financial institutions. Because of real-time settlement, it enables business process re-engineering in a borderless market to achieve zero latency, resulting in improved customer service levels and risk management. It has had exceptional growth since its inception in the 1990s.

The rate of growth in Developed Countries is higher, while it is lower in LDCs. With the passage of time, the concept of internet banking has gained popularity in India. Most banks have already introduced e-banking services, as these services benefit both banks and consumers. Banks are confronted with numerous obstacles, but they also provide numerous opportunities. ATMs, credit cards, RTGS, debit cards, mobile banking, and other financial advances have fundamentally transformed Indian banking. As a result, the industry has shifted from a seller's market to a buyer's market, causing bankers to adjust their approaches from "traditional banking to convenience banking" and "mass banking to class banking." The move has also made it easier for the average person to bank for a range of demands and requirements. E-banking will not only be an accepted means of banking in the future, but it will also be the preferred mode of banking of customers.

It has had a substantial impact on strategic business concerns for banks by remarkably lowering delivery and transaction costs. Developing countries confront numerous hurdles to the successful implementation of e-banking programs when compared to developed countries. With low and insufficient security, infrastructure, and internet penetration, it is critical to take the essential steps to improve E-banking.

[112] ibid
[113] ibid

CHAPTER 3

CYBER CRIME IN THE INDIAN BANKING INDUSRTY

3.1INTRODUCTION

Banking is one of the most important institutions in any society, and the protection of bank customers is critical to the country's well-being. Banks have been exposed to a variety of dangers. The advancement of computers has had a significant impact on the banking industry, but it has also increased the number of ways in which people might become victims of various attacks. The primary concern for financial institutions in the twenty-first century is the explosive increase of cybercrime. Criminals have used telephone lines to perpetrate crimes on occasion during the beginning of the 1970.[114]

In the past few years, several reports of cyber fraud in Indian banking sector have been registered. Although banking frauds have long been considered a cost of doing business in India, since liberalization, the incidence, complexity, and cost of banking frauds has increased dramatically, posing a severe threat to regulators such as the RBI. RBI defines fraud as "a deliberate act of omission or commission by any person, committed in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting in wrongful gain to any person for a temporary period or otherwise, with or without monetary loss to the bank."[115]

“Public sector banks (PSBs)” in India have lost a total of Rs. 22,743crore in the last three years due to different banking frauds. Furthermore, the increased amount of online transactions, along with the lack of robust cyber security mechanisms, gives fraudsters room to operate. According to a media source, a total of Rs 615.39crore was stolen in more than 1.17lakh cases of online banking in India between April 2009 and September 2019. The number of banking fraud cases has decreased as a result of the RBI's different actions, but the amount of money lost has climbed in recent years. An initial inquiry into these incidents found that not only midlevel staff, but even high

[114] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 466

[115] Rajib Bhattacharyya, 'Information Technology and Cyber Law: A Globalized Review' (2018) 9 Indian JL & Just 115

managers were involved, as seen in the cases of Syndicate Bank and Indian Bank.[116] The involvement of bank workers in the cyber fraud emerges serious concern about the efficiency of corporate governance at these banks' top levels. Furthermore, non-performing assets (NPAs) have been on the rise, particularly among PSBs, putting their profitability at risk. Risky NPAs have been linked to a number of factors, including global and domestic slowdowns, but there is also evidence of a link between frauds and NPAs. [117]

The stability of a country's banking and financial system influences its ability to produce and consumes goods and services. It is a direct reflection of the citizens' well-being and living standards. As a result, if the banking system is troubled by large levels of NPAs, it is cause for concern, as it indicates financial distress among borrowers or inefficiencies in transmission channels. These are the problems due to which now Indian economy is suffering to a great extent.[118]

ATM, money laundering, and credit card fraud have been the most common types of fraudulent attacks. The main goal of these assaults is to gain access to a user's bank accounts and funds in such a way that the attacker controls the cash without the user's awareness. Cyber criminals may utilize banking passwords such as PIN, password, certificates, and others to get access to banks and steal enormous sums of money in certain cases, while in others, they may attempt to take all the money and move the funds to mule accounts. Cyber attackers frequently seek to harm a bank's reputation before blocking bank servers, preventing customers from accessing their accounts. [119]

3.2CONCEPT OF CYBER CRIME

Today, internet activities are not confined to technology geeks for technical objectives; rather, every second person is taking use of the ease internet availability and accessibility for everyday purposes such as banking, e-commerce, education, entertainment, and many more. The proliferation of smartphones has unquestionably functioned as a fuel for this phenomenal internet expansion.

[116] Debasree Saha, "Cyber Laws and Banking Frauds with Special Reference to Private and Public Sector Bank in India (2016) 3 Int'l J Adv Res Fdn 10
[117] Charan Singh, "Frauds in the Indian Banking Indusrty" (2016) 505 IIMB 2
[118] ibid
[119] ibid

The IT Act or IPC does not define cyber crime, although it does have penalty provisions for cyber crime. In simple terms, the term "cyber crime" means any crime involving a computer and a network. Cyber crime is viewed as a serious crime or danger to all elements of a country's economic prosperity with the majority of incidents occurring in financial institutions. Credit card fraud, spamming, spoofing, e-money laundering, ATM fraud, phishing, identity theft and denial of service are all examples of cyber crime.[120]

According to Douglas and Loader (2000), cybercrime is defined as computer-mediated acts carried out through worldwide electronic networks that are either illegal or deemed illegitimate by some parties. Banking frauds are cybercrimes perpetrated using online technology to fraudulently remove or transfer money from one account to another in the banking sector (Wall, 2001). According to Wall (2001), cybercrime can be divided into four categories: deceptions, pornography, violence, and trespass. Banking frauds are classified as cyber-deception, which is defined as unethical behaviors such as stealing, credit card fraud, and intellectual property infringement.[121]

Cyber crime is defined as the unauthorized use of computers and the internet. It is an illegal activity where the intruder steal someone's identity or sell contraband, stalk victims or disrupts operations with malicious software by using computer and the internet.

Any criminal conduct involving computers and networks is classified as cyber crime commonly called hacking. Cybercrime also covers classic crimes that are carried out over the internet. Hate crimes, telemarketing and internet fraud, identity theft, and credit card account thefts, for example, are all considered cyber crimes since they include the use of a computer and the internet. In other words, offenses committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as the Internet, email and mobile phones are defined as cyber crime.[122]

A broad definition of cyber crime could include any illegal activity in which a computer is used as a tool, a target, or both. Financial crimes, the sale of illegal goods,

[120] [120] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 468

[121] ibid

[122] ibid

pornography, online gambling, intellectual property theft, e-mail spoofing, forgery, cyber defamation, and cyber stalking are all examples of how the computer can be utilized. However, given the following scenarios, all computers could be used to commit illegal crimes,[123] viz-

Unauthorized access to computers/ computer system/ computer networks, theft of information contained in electronic form, e-mail bombing, data diddling, salami attacks, logic-bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Cybercrime is a type of crime that takes place in cyberspace, or in the realm of computers and the internet.

Cyber space refers to the virtual world created by mankind via the use of computers and networking, in which people interact and exchange information using a variety of languages or communication protocols devised by humans to allow one machine to communicate with another. William Gibson conceived the cyberspace in his science fiction novel 'Neuromancer.'

Cybercrime has had an impact on the banking sector as well. 'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank,' according to the Reserve Bank of India.[124]

As per the Zee Research Group (ZRG) , the Indian Banking Industry grew at an average pace of 18% over the last decade, compared to a GDP growth rate of 7%. During the same time span, however, cyber crime in the banking industry has considered as a major issue and source of concern for the banking industry.

“Relevant security mechanisms have not been followed by the private sector banks while public sector banks have continued to follow the old approach,” said Pavan Duggal, a cyber law expert, explaining why the amount related to cyber crimes has increased. He bemoaned the lack of adherence to the Gopalakrishna Working Group's (GGWG) report recommendations on safe electronic banking. These recommendations stipulated that each bank establish a separate information security function dedicated solely to information security management, that a Board-approved

[123] ibid
[124] ibid

information security policy be in place and reviewed at least once a year, and that digital evidence be treated in the same way as any other form of legal proof.

3.2.1 HISTORY OF CYBER FRAUD IN INDIAN BANKING SECTOR

In the year 1820, the first cybercrime was documented. That's remarkable given that the Abacus, which is regarded to be the earliest form of computer, has been around in India, Japan, and China since 3500 B.C. The era of modern computers, on the other hand, began with Charles Babbage's analytical engine. The new loom was invented by Joseph Marie Jacquard, a French textile maker, in 1820, and his employees feared losing their employment. They carried out acts of sabotage in order to prevent Jacquard from using the new technology in the future. This is the first time a cyber crime has been documented.[125]

The case of Yahoo v. Akash Arora was one of the earliest examples of cyber crime in India. This incident happened in 1999. The defendant, Akash Arora, was accused of utilizing the trademark or domain name 'yahooindia.com,' and a permanent injunction was sought in this case. The case of Vinod Kaushik and others v. Madhvika Joshi and others is the other. According to section 43 of the IT Act, 2000, accessing the e-mail accounts of the spouse and father-in-law without their permission is prohibited. In 2011, a decision was reached in this matter. All of these instances deal with the question of how cyber crime has evolved, with a focus on India.[126]

In the 1980s, a basic computer virus kicked off the evolution of cyber-attacks. Viruses are self-replicating computer programs that change other programs and insert their own code in order to infect the system. With some applied research in the late 1990s, hacking websites evolved as a danger to systems. [127]Malicious code as an attack emerged in 2004, posing a threat to application security that could not be managed by

[125] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 468

[126] Rajib Bhattacharyya, 'Information Technology and Cyber Law: A Globalized Review' (2018) 9 Indian JL & Just 115

[127] Varsha, 'An Analysis on Cyber Crime' < https://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html > accessed June 25 2021

traditional antivirus alone. Attack scripts, viruses, Trojan horses, worms, and harmful material are all examples of these codes, which represent a broad range of system security terminology. Due to the accelerated development of attacks, complex Trojans and worms emerged in late 2008, followed by identity theft and phishing attempts in 2012. Then, in late 2015, attackers evolved with substantial threats such as DOS and DDOS attacks, and later in 2015, cyber espionage and cyber warfare became extensively employed as a sort of attack, until now. Due to the use of several internet connections, DDOS assaults are more widespread and hazardous than DOS attacks, and victims are unable to identify the source of the attack.[128]

As social networks became more prominent, the rate of cyber crime began to rise as thieves gained easier access to the user's personal life. As a result of this growth, one of the most heinous types of criminality emerged: non-consensual sharing of intimate images (NCSIA). In 2015-2016, 569 incidents out of 5987 cybercrime cases were motivated by sexual exploitation, according to the National Crime Record Bureau.

In such circumstances, obscene photographs of the victim are posted on the internet without the victim's knowledge or agreement. [129]Non-consensual porn is another name for it.

According to NCRB data, the dissemination of such photographs on the internet has surged by 104 percent in recent years. Most of these crimes go unreported since the victim's family does not want to interrupt their privacy or become involved with the police and courts, and more importantly, the victim prefers to keep such cases to herself/himself for fear of being blamed. The perpetrator is aware of these realities and exploits them.

This is a crime that can traumatize whoever is victimized, whether it's a great star, such as Hollywood actress Bella Thorne, or a regular girl. It is a major issue in India, which should be concerned about because there are no specific laws dealing with such crimes. Perhaps because the majority of cases go unreported, legislators are unaware of the severity of the crime. If such a case arises, we have a few laws under the Indian Penal Code (IPC) and the Information Technology Act to help us deal with it.[130]

[128] ibid
[129] ibid
[130] ibid

3.2.2 TECHNIQUES OF CYBER INFRINGEMENT IN BANKING SECTOR

Digital wrongdoing can simply be defined as the use of a computer and a network as a channel, source, instrument, target, or location for wrongdoing. The financial misbehavior has drifted towards the advanced world with the growing part of web-based commerce and e-exchanges. Digital wrongdoings are on the rise all across the world, and in recent years, India has seen a significant increase in instances involving digital infractions.

Cyber fraud in Indian Banking Industry could be classified into two categories i.e. direct fraud and indirect fraud. Credit/Debit card fraud, employee embezzlement, money laundering and salami attack are example of direct fraud. Whereas indirect fraud includes phishing, pharming, hacking, virus, spam, advance fee and malware. The types of cyber fraud in Indian banking industry are briefly discussed below –

1. **Credit/Debit Card fraud –**

   Identity theft and credit card/debit card fraud are two types of e-fraud that are interchangeably use. It entails impersonating someone else and stealing their identity (name, SIN, credit card number, or other identifying information) in order to commit fraud. It is the fraudulent use of a credit/debit card to obtain money or property without the credit/debit card owner's knowledge. Theft of a person's identity can occur in a variety of ways. Skimming is when someone steals information from a credit card while it is being used for a genuine purchase. This kind of scheme normally takes place in a store where the customer's credit card is removed out of sight while the transaction is being processed. The card will be swiped through an electronic device called a "wedge" or "skimming device," which records all of the information on the magnetic strip. Offenders may use sophisticated methods to collect credit card information, such as hacking into merchant databases or simply “engineering” victims into providing their credit card information.[131]

2. **Salami Attack –**

   In terms of information security, a salami attack is a series of tiny attacks that culminate in a large strike. A salami attack is a huge attack that is undetectable due to the existence of this type of cybercrime when several tiny attacks sum up to one.

[131] Seema Goel, “Cyber Crime: A Growing Sector in India Banking Sector” (2016) 4 ICRISTME 13

Salami cutting is a term used to describe this process.[132] And, while being sliced into salami is frequently employed for the success of criminal activities, it is simply a tactic for gaining advantage over time by accumulating it in little increments. Customer records, such as bank and credit card numbers, are captured via an online database, and the hacker can only deduct a little amount from both accounts over time. Customers are unaware of the cutting, therefore no report is filed, allowing the invader to remain undetected.

Salami attack can be categorized into two types – Internal attacks and External Attacks.

Internal Attacks - This is the most common type of Salami assault, in which someone who knows the enterprise's security mechanisms tries to loot it and cause severe damage. (Internal attacks) When, for example, an accountant with a single bank interacts with the bank's clients on a regular basis.

External Attacks - External assault is a sort of Salami assault that occurs outside of the organization, as the name implies. An external attack is one in which the attacker leaves the firm and then attempts to steal the company's expertise while causing considerable harm. Salami assault is frequently referred to as a fragmented Nazi party strategy.

3. **Phishing –**

"Phishing" is a type of online fraud that involves obtaining personal user information such as logins and passwords. This is performed via sending out mass emails on behalf of well-known brands, as well as personal messages through other services, such as banks or social media networks. Phishers today are mostly interested in obtaining information from users regarding their credit cards and accounts. Due to the growing number of electronic banking transactions and online shopping, phishing is one of the most popular means of fraudulent behavior with payment cards on the Internet.[133]

When a letter has a direct link to a website that is externally difficult for the user or customer to differentiate from the genuine one or a website with a redirection, it is

[132] ibid

[133] Miss Neeta & V. K. Bakshi, "Cyber Crimes in Banking Sector" (2019) 6 AIIRJ 25

fairly common. After a user visits a phony page, fraudsters attempt to persuade them to input their username and password on the fake page, which they then use to access the cabinet on the website, allowing fraudsters to access their accounts and bank accounts. [134]

One of its specific phishing strategies is to do a direct search for a victim in order to obtain confidential information such as a victim's bank card number and personal information. The examined type of fraud is distinguished by the fact that the victim is a participant in the perpetrator's crime. By researching typical types of victim's behavior, personal qualities, and other factors, significant reductions in potential dangers for the broader community can be achieved. Psychological and socio-demographic variables, as well as online routine assessments, should all be included when predicting victims. It is common that most of the cyber victims are older due to their lack of intellectual development, inexperience with the internet, credulity, absent mindedness and inattention.[135]

In 1987, a detailed description of phishing was published, and the term "phishing" was first used in 1996. The term refers to "baits" that are employed in the hopes that a potential victim will "bite" by clicking on a malicious link or opening a malicious attachment, allowing their financial information and passwords to be taken. A false website isn't required for every phishing effort. Users should telephone a phone number if they have problems with their bank accounts, according to messages claiming to be from a bank. When the user dials the phisher's phone number (which is provided by a Voice over IP service), the user is prompted to enter the account number and PIN. Vishing (voice phishing) makes use of bogus caller-ID data to make it appear as if the call is coming from a legitimate company.[136]

PROTECTION AGAINST PHISHING

a) Email messages requesting personal information should be avoided at all costs. It's quite improbable that your bank account will send you an email requesting this information. Companies that are legitimate do not seek for personal information by email or text. Delete emails or text messages

[134] ibid
[135] ibid
[136] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 601

requesting confirmation or information such as credit and debit card numbers, bank account, adhar card numbers, and passwords. [137]

b) If you don't react, the message may look to be from a company you do business with, such as a bank, which may threaten to terminate your account or take other action if you don't respond. Don't respond, don't click on links, and don't call the phone numbers provided in the message. These messages directed you to spoof sites that appeared to be legitimate but were designed to steal your personal information so that a scammer could rack up bills or commit crimes in your name. As a result, never fill out a form in an email message that requests personal information. [138]

c) Area codes can often be deceiving. To update your account or get a refund, some scammers will require you to call a phone number. A local area code, on the other hand, does not guarantee that the caller is local. [139]

d) Any unusual activity should be immediately reported to your bank. Call the number on your financial statement or on the back of your credit card if you have questions about your account or need to contact a company with which you do business. [140]

e) Instead of clicking on a link in an email message to go to a web page, type the URL into your browser. [141]

f) Check your financial accounts (including debit and credit cards, bank statements, and so on) on a regular basis to ensure that the transactions mentioned are genuine. [142]

[137] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 603

[138] ibid
[139] ibid
[140] ibid
[141] ibid
[142] ibid

4. **Vishing–**

   "Vishing" is a combo of voice and phishing in which cyber criminals make voice calls to impersonate bank workers, causing bank customers to divulge all account information.[143]

5. **Smishing –**

   "Smishing" is a combo of text messaging and phishing. It is similar to vishing in that cyber criminals collect bank information from clients by sending SMS and convincing them that the message is authenticated by the banks.[144]

6. **Credit Card Redirection –**

   Credit card redirection is new form of cyber fraud. This new form of cyber assault affects e-commerce websites, giving hackers access to the users' credit card information. When utilized in a specific e-commerce website, the credit card processing file is modified, and the details of such credit cards are redirected to a phishing site during the payment process.[145]

7. **Hacking –**

   Hacking is a crime that involves a person gaining unauthorized access to a system or attempting to circumvent security features by hacking into consumers' banking sites or accounts. The updated IT Act, does not define hacking. A hacker, however, can be penalized under Section 43(a) of the Information Technology (Amendment) Act, 2008, read with Section 66 of the Information Technology (Amendment) Act, 2008, and Sections 379 and 406 of the Indian Penal Code, 1860. Before the 2008 Amendment Act, hacking was punished by up to three years in prison or a fine of up to 2lakh rupees, or both, under Section 66 of the IT Act. If the crime of hacking is proven, the accused may be sentenced to three years in prison or a fine of up to 5lakh

[143] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 605

[144] ibid

[145] ibid

rupees, or both, under the IT Act. Hacking is not only a cognizable offense, but it is also Non-Bailable offense.[146]

8. **Fraud of Credit Card –**

Customers use their credit card or debit card for any online payment, and another person, with malafiade intentions, hacks and misuses the card data and password for online purchases using the customers hacked card credentials or commits a fraud. When electronic transactions are not secured, the hacker can use the credit card by impersonating the credit card owner.[147]

9. **Key logging –**

Fraudsters utilize key logging to keep track of actual keystrokes and mouse clicks. Key loggers are "Trojan" software applications that target the operating system of a computer and are "installed" by a virus. Because the fraudster collects the user ID and password, as well as the account number and anything else typed, these can be very harmful.[148]

10. **Viruses –**

A virus is a program that infects an executable file and causes the file to behave abnormally after infection. It spreads by attaching itself to executable files such as program files and operating systems. Running the executable file could result in additional copies of the virus being created. Worms, on the other hand, are programs that can copy themselves and send copies to other computers from the victim's computer. Worms do not alter or destroy any files; instead, they multiply and transmit copies to other computers from the victim's computer.[149]

11. **Spyware –**

Spyware is the most common method of stealing internet banking credentials and using them for fraudulent purposes. Spyware collects data from the computer or when it is being transported between the computer and websites. It is frequently installed using fraudulent "pop-up" adverts requesting the download of software. Antivirus software that is industry standard detects and removes this type of malware, usually by preventing the download and installation before it infects the computer.[150]

---

[146] ibid
[147] Harshita Rao, “Cyber Crime in Banking Sector” (2019) 7 Int’l J Res Granthalaya 148
[148] ibid
[149] ibid
[150] ibid

12. Watering Hole –

Cyber fraud known as "watering hole" fraud is a branch of phishing attempts. A harmful code is injected onto public web pages of a website that is only frequented by a small number of people at a watering hole. When a victim visits a site that has been injected with malicious code by attackers, the attacker is able to track down the victim's personal information. In a phishing assault, the victim unwittingly gives up personal information, but in a watering hole attack, the attacker waits for the victim to visit the site. When there is greater usage and exploitation of zero-day vulnerabilities in various software products like Adobe Flash Player or Google Chrome, there may be an increase in watering hole events. Cyber criminals at a watering hole utilize black market kits to infect, inject, and configure a website that may be new or updated in order to entice visitors to disclose personal information. The attackers normally compromise the site that will be used in the attack months before the actual attack. To carry out such an act, they employ expert methods. As a result, cyber-crime cells have a hard time locating corrupted websites. Watering hole is a type of surgical attack in which hackers target a select set of users on the internet, and it is less annoying than phishing.[151]

13. Pharming –

The terms "farming" and "phishing" are associated with pharming. When a customer logs in to a bank's website, the attackers hijack the URL in such a way that they are led to another website that is fraudulent yet looks like the bank's original website. “Pharming takes place through the internet, and ATM skimming is another method. In other words, cyber criminals hack the URL of a bank's website, diverting the user to a bogus bank website. Customers will find it difficult to tell the difference between a genuine and a phony website, therefore they will often provide their information on such sites.[152]The URL of a bank can be hacked in two ways:

a) DNS cache poisoning
b) Hosts file modification

[151] Miss Neeta & V. K. Bakshi, “Cyber Crimes in Banking Sector” (2019) 6 AIIRJ 25

[152] ibid

14. DNA Cache Poisoning –

DNS servers are used in a company's network to speed up resolution response times by caching previously obtained query results. Poisoning attacks on DNS servers are carried out by exploiting a flaw in DNS software. As a result, the server validates DNS replies erroneously, ensuring that they are from an authoritative source. Incorrect entries will be cached locally by the server and served to other users who make the same request. Bank users might be sent to a server controlled by criminals, which could be used to spread malware or trick bank customers into providing their credentials to a spoof of a legal website. An attacker can hijack consumers by spoofing an IP address; DNS entries for a bank website on a certain DNS server and replacing them with the IP address of a server they control. [153]

15. Malware Based Attacks –

One of the most dangerous cyber risks to electronic financial systems is malware-based attacks. A malicious code is created in such attacks. The amount of malware attacks in the banking sector is on the rise these days. Carbep, Tinba, Spyeye, Zeus, and KINS are some of the most well-known banking malware. The malware known as Zeus is the eldest of the bunch. It was discovered in July 2007 when information from the US Department of Transportation was lost and stolen. There have been other malwares detected in prior years that have been used to commit large-scale bank fraud. [154]Almost every virus has two characteristics: one, it secures a backdoor entry into the system, and the other, it steals a user's credential information.

3.3 IMPACT OF CYBER FRAUD ON BANK'S FINANCE

The sorts of cyber-deception include frauds in the e-banking sector. In addition, cyber-deception is defined as an immoral action that involves theft, credit card fraud, and intellectual property infringement. The majority of frauds are conducted for two reasons: first, to get access to the user's account and steal personal information, and second, to move monies from one account to another. The second method is to smear

[153] ibid
[154] ibid

the bank's image by blocking the bank server, preventing the customer from accessing his account.[155]

Because of the rise in cell phones with internet access, incidences of cybercrime have become more heinous. Cell phones are being used for a variety of internet activities such as saving money online, buying online, and paying service fees, and they are frequently used by criminals to gain access to personal information. Financial gain has consistently surpassed other goals such as retribution, extortion, and political purposes among the different motivations for committing cybercrime for many years. Alarmingly, simple phishing attacks have a 45 percent success rate due to a lack of awareness about the standard safeguards in place to protect against clever digital criminals.[156]

The main issue of concern here is that there is absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks (Stafford, 2013).

High profile banks in the UK like Barclays and Santander were targeted by hackers who stole personal information of nearly 2.9million credit card customers by hacking the software maker system of these banks, which led them to incur huge losses. However, such attacks have occurred in the United States as well in recent years, and in order to mitigate the impact, they developed the program Quantum Dawn 2, which tests the efficacy of systems deployed in banks in reaction to cyber-attacks (Stafford, 2013).[157]

However, the sad reality is that most systems lag behind the instruments used by cyber thieves, necessitating the construction of a flexible system capable of meeting and defeating incoming attacks. The hour before, during, and after an attack, a good defense system to resolve the attack is required.

[155] A. R. Raghaban & Latha Parthiban, "The Effect of Cyber Crime on Bank's Finanance" (2014) 2 Int'J.Curr.Res.Aca.Rev 173
[156] ibid
[157] ibid

In 2014, there were 3855 cyber crimes committed for monetary gain (NTRO) and 534 phishing incidents (CERT-In), indicating the breadth of cyber crime. These episodes only cover the details of what happened; they don't include what happened that was either unreported or went ignored.[158]

Banks all over the world are increasingly becoming practical targets of distributed denial-of-service (DDoS) attacks, which are sometimes used as part of a scheme to divert security professionals' attention away from the draining assets, while doing something else dangerous in parallel, such as adding malware or messing with IT resources. Cutting edge Constant Danger, a type of implanted hacking endeavor with a hidden plan, is the most current child on the block, with improved multidimensional character and adroitness.[159]

When the aggressors are unable to produce any important data, they destroy the bank's website as a form of retaliation for their failed endeavors. Aside from the financial gains from successful digital assaults, the presence of online illegal companies commonly referred to as the "Darkweb" contributes to the inspiration of committing cyber crimes as a standard for exchanging personal data, new undertakings, and perfected hacking units. In these online extortion networks, sensitive data such as stolen/spilled Master card details, web-based managing an account accounts, treatment records, and authoritative access to servers is swapped for cash.[160]

3.4 Cyber Fraud Safety Mechanisms in the Banking Sector

Our economy's backbone is the banking industry. The rising number of cyber-crime cases has resulted in significant economic losses. Cyber-attacks should be avoided by ensuring that appropriate law is in place and that it is followed. Both the banks and the customers should be made aware of the risk and the precautions that should be taken. To combat cybercrime, collaboration amongst diverse parties is required.[161]

[158] Harshita Rao, "Cyber Crime in Banking Sector" (2019) 7 Int'l J Res Granthalaya 148
[159] ibid
[160] ibid
[161] Miss Neeta & V. K. Bakshi, "Cyber Crimes in Banking Sector" (2019) 6 AIIRJ 25

The Indian government formed an Inter Departmental Information Security Task Force (ISTF), with the National Security Council serving as the nodal agency for all matters relevant to the effective implementation of its cyber security strategy. The Indian Computer Emergency Response Team (CERT-In) is a national nodal organization tasked with responding to computer security events. Coordination of responses to security incidents and other major events; issuance of advisories and time-bound advice regarding imminent threats; product vulnerability analysis; conducting trainings on specialized topics of cyber security; and evolution of security guidelines on major technology platforms are just a few of the activities undertaken by CERT-In in implementing cyber security.[162]

Banks should implement a variety of security measures to protect themselves and their customers against suspected cyber-attacks. A penetration test is carried out at bank premises to figure out flaws in the system and detect breaches in which the tester acts as an intruder and attempts to break the security system in order to test the security of the network and infrastructure of banks**.** A variety of such tests have been conducted in the past, and the results show that web application vulnerabilities, poor network security, inefficient password management, improper server configuration, and a lack of knowledge account for the majority of vulnerabilities detected in Indian banks.[163]

Cyber attacks are evolving in tandem with the advancement of technology. To obtain privilege and disrupt the network, attacks have gotten more competent at researching and accumulating weakness and locating flaws in the system. Banks are now adopting the latest cyber security and technology and are willing to spend more money to secure their environment from unauthorized access and unwanted data and security breaches in order to become more aware of and advanced with the latest hacking modus operandi. The banking sector can be protected against unwanted attacks by properly configuring and maintain a firewall. Banks should implement a variety of security measures to protect themselves against known cyber-attacks. [164]

---

[162] ibid
[163] ibid
[164] ibid

A penetration test is carried out at bank premises to figure out flaws in the system and detect breaches in which the tester acts as an intruder and attempts to break the security system in order to test the security of the network and infrastructure of banks. A number of such tests have been conducted in the past, and the results show that web application vulnerabilities, poor network security, inefficient password management, improper server configuration, and a lack of knowledge account for the majority of vulnerabilities detected in Indian banks. [165]

Certain safeguards, such as the usage of the secret socket layer (SSL) protocol, are required to avoid cyber-attacks on bank backend online services. When a browser requests access to a website's data, it first fetches the SSL certificate and verifies that it is not expired, that it was issued by browser-certified authorities, and that it is being used by the website for which it was issued. If all of these conditions are met, the browser is granted access. [166]

Ineffective password management can make it easier for attackers to get access to the network and server levels. Passwords must be maintained secure, changed at regular intervals, monitored, and stored in a secure, encrypted manner. At every level of security, password encryption is required. Passwords should be adequately secured and not exposed anywhere in the system. Any password should be accessed via encryption and decryption techniques.[167] Wherever passwords are hardcoded, they can be encrypted in a configuration file, which can subsequently be used to access passwords throughout the code.

This configuration is simple to implement in order to better protect source code from tampering. The use of two-factor or multi-factor authentication is a better technique to deal with login issues. Firewall settings must be used to protect networks. To defend the system core, multiple tiered protection frameworks should be suggested, as depicted in the diagram above. Firewalls and traffic content filters at the top network layer are required to prevent unauthorized and undefined data from entering the network. [168]Antivirus software should be used to guide the platform layer underneath that. Old software and hardware should be replaced with newer versions with better

[165] ibid
[166] ibid
[167] ibid
[168] ibid

security fixes, and the operating system and other applications should be patched and upgraded on a regular basis. The backbones of back office IT are the application layer's many lines of source codes. To secure the source codes, a necessary preventative system must be implemented. To protect their codes, developers must use password encryption and reduce code-related risks. For auditing purposes, files and data must also be encrypted and safeguarded in a secure manner. [169]

A survey of a few Indian banks was conducted to determine the safety precautions they took to protect the environment. Most banks have implemented password encryption and other prevention measures mentioned above, but there are minimal user awareness programs found where a small group of people were surveyed with a set of questions related to cyber security, but the results showed that only 5-10% [170]of people were aware of policies and security awareness, with the majority having little or no knowledge.

Banks should focus on teaching staff through self-awareness programs, offering training on data protection regulations, and arming them with cyber security expertise, so that they are always on the lookout for any form of external intrusion. Users of online banking should use extra caution when doing daily transactions online. More than 60% of customers are uninformed of the underlying information security vulnerabilities involved in banking processes/transactions, according to data collected from reports. Furthermore, approximately 55% of customers are unable to exercise extra caution when using online banking services. A few common preventive measures are listed below as part of a user awareness program that all bank personnel must undertake[171] –

- For network share login accounts, use a strong and unique password. Delete any shares that are no longer in use. [172]
- Instead of exposing remote desktops, use a Virtual Private Network (VPN) for all remote work (RDP). [173]

[169] Seema Goel, "Cyber Crime: A Growing Sector in India Banking Sector" (2016) 4 ICRISTME 13
[170] ibid
[171] ibid
[172] ibid
[173] ibid

- In working directories, shared software should not be retained in exe format. Only after IT Security approval may you download from a safe source when you need it.
- Tracking RDP access and turning it off when not in use.
- Consistently keep your browser up to date, and block all add-on pop-ups.
- Verification of the genuineness of the accessed browsing site in a timely manner. In addition, any suspicions should be immediately reported to the bank's IT security.
- To avoid connecting to phishing sites, bookmark crucial websites.
- Personal information should not be shared on any unfamiliar websites.
- Increasing the security of e-mail in order to detect malicious attachments. Multifactor authentication is enabled for legitimate access.
- Examining every email sent to the bank. Avoid opening emails from unknown senders and report them to the bank's phishing department.
- Assuring that security software and the operating system are patched at regular intervals.
- When not in use, the webcam should be covered.
- Data should be backed up on a regular basis and stored in a secure location. IT Security should not share sensitive information on any platform that has not been vetted or safeguarded.

There are some other crucial cyber fraud safety mechanisms which must be followed, viz. –

1. **Encryption of password –**

Passwords are one of the most significant security elements utilized today. It is critical for users to have passwords that are both secure and strong. Most contemporary Linux distributions contain password applications that prevent users from creating passwords that are easily guessable. The user must ensure that the password program is current and includes these features. Encryption is extremely beneficial, if not essential, in today's world. Encrypting data can be done in a variety of ways, each with its own set of properties. To encrypt passwords, most Unixes (including Linux) rely on a one-way encryption mechanism known as DES (Data Encryption Standard).The database then stores the encrypted password. When a user attempts to

log in, the password they enter is encrypted once again and compared to the record in the password file. The database then stores the encrypted password. When a user attempts to log in, the password they enter is encrypted once again and compared to the record in the password file. If they're the same, it's the same password, and access was granted. Although DES is a two-way encryption technique (with the appropriate keys, a user can code and then decode a message), most Unixes employ a one-way variation. This means that reversing the encryption to extract the password from the database's contents should be impossible.[174]

2. **Virtual keyboard –**

A virtual keyboard is a computer keyboard that a user uses instead of hitting actual keys by typing on or within a wireless- or optical-detectable surface or region. A system like this can give a user of a small handheld device like a cellular phone or a PDA (personal digital assistant) complete keyboard functionality. The keyboard is projected optically on a flat surface in one technique, and when the user presses a key, the optical device recognizes the stroke and communicates it to the computer. The keyboard is projected on an area in another technology, and selected keys are communicated as wireless signals utilizing short range Bluetooth technology. The keyboard could theoretically be projected in space and the user could type by moving fingers through the air with either approach. A soft keyboard that appears on a display screen as an image map is also referred to as a virtual keyboard. A software-based keyboard can be altered in some instances.

3. **Secured Socket Layer (SSL) –**

Secure Sockets Layer (SSL) is a set of cryptographic methods for securing Internet communication. SSL is the standard security system to connect a web server to a browser with an encrypted link. This link ensures the privacy and completeness of all data passed between the web server and the browser. In order to protect their online transactions with its customers, SSL is an industry standard that millions of websites use. A web server requires SSL certificates in order to create an SSL connection. Users will be asked to answer a number of questions concerning the identity of the

[174] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 610

Website and the company when choosing to enable SSL in a Web server.[175] The web server then generates a Private Key and a Public Key cryptographic key pair. The Public Key does not need to be kept secret, and it is stored in a Certificate Signing Request (CSR), which is a data file that also contains the information. After that, the user must submit the CSR. The Certification Authority will validate the details throughout the SSL Certificate application process and issue an SSL Certificate including the details and allowing the user to utilize SSL. The issued SSL Certificate will be matched to the Private Key by the web server. The web server will then be able to create an encrypted link between the website and the web browser used by the customer. Customers are unaware of the complexity of the SSL protocol. Instead, their browsers provide a key indicator that they are currently secured by an SSL encrypted session - the lock icon in the lower right-hand corner, which when clicked displays the SSL Certificate and its contents. All SSL Certificates are provided to corporations or persons who are legally responsible. An SSL Certificate will often include the following information: domain name, firm name, address, city, state, and country. It will also include the Certificate's expiration date as well as information about the Certification Authority that issued the Certificate. When a browser connects to a secure site, it retrieves the site's SSL Certificate and verifies that it has not expired, was issued by a Certification Authority that the browser trusts, and is being used by the website for which it was issued. If any of these checks fail, the browser will display a warning to the user, informing them that the site is not protected by SSL.

4. **SMS Alerts –**

SMS evolved from radio telegraphy in radio memo pagers utilizing established phone protocols, and was later defined as part of the Global System for Mobile Communications (GSM) series of standards in 1985 as a means of sending messages of up to 160 characters to and from GSM mobile handsets. The abbreviation SMS stands for short message service. An SMS alert is a message sent to a cellular device, such as a phone, to alert the recipient of a certain event. A text message is received in the same way that a phone call is. When a message is received, it is usually indicated by a sound or vibration. [176]People can opt up to get several types of SMS alerts.

[175] ibid
[176] ibid

Appointment reminders, financial transactions, and promotions or sales offered by establishments they frequent are examples of these. An SMS alert is frequently sent to a large number of recipients at once. [177]

This means that if two persons are set to get the same SMS alert at the same time, they should get it around the same time. Personal information-containing SMS alerts, such as banking transactions or payment requests, are normally not handled this manner. Sending an SMS alert is frequently considered as a service by the sender. In many circumstances, the senders of such letters do not charge the recipients. However, the sender and receiver's cellular operators may levy a cost to both parties. An SMS alert can also be included as part of a subscription in some situations. This is a service in which a person pays a charge in exchange for receiving specific types of notifications. News, sports, and weather updates are examples of these.[178]

5. **Programs for User Awareness –**

The user or customer is the essential component of any field. We can create a lot of software or technology to safeguard things, but it's all for shrink if the end user doesn't have the right information about it. New gadgets and technologies are being introduced into the banking sector on a daily basis, allowing the bank to deliver secure transactions to end users. The banks must also run some awareness programs for end users using these gadgets so that they may comprehend the concept of secure transactions as well as learn how to utilize these gadgets for secure transactions.[179]

3.5 RISE IN CYBER CRIME AND REASONS BEHIND IT

As a result of digital transformation and the use of new technology, the banking industry is better able to service its consumers. These are hardly unmixed gifts, and they bring new challenges for banks with them.

The banking industry invests a significant amount of money on cyber security solutions and maintaining a strong IT infrastructure. Cyber criminals, on the other hand, are developing new methods for breaking into bank networks.

[177] ibid
[178] ibid
[179] ibid

Since hackers successfully stole approximately USD 100 million from Bangladesh's central bank in February 2016, fears of a big cyber attack on banks have grown. Hackers stole more than USD 31 million (two billion roubles) from the Russian central bank and commercial banks shortly after that incident, according to Russian central bank officials. In July 2016, the Union Bank of India was again the target of an attack.[180]

Its Nostro Account was robbed of roughly USD 171 million by cyber criminals. Using spoofed RBI IDs, the attackers allegedly acquired access through spearphishing.

In February 2018, a cyber assault penetrated the SWIFT messaging system, resulting in payment instructions being issued to various banks in multiple jurisdictions, stealing around USD 2 million from City Union Bank accounts. The bank discovered the transactions while reconciling accounts, and it was able to recover nearly half of the money. [181]

In 2017, India recorded 21,796 cyber offences, up 77 percent from 2016. The number increased to 27,250 in 2018. Due to a lack of awareness regarding cybercrime and classification methods, the true numbers could have been far higher. The majority of cyber crimes were classified as ATM fraud, followed by internet banking fraud. The states with the most cases were Karnataka and Maharashtra. [182]

Criminals were carrying out targeted attacks on financial institutions like banks, according to a research by renowned cybersecurity vendor Kaspersky. Small banks are the primary targets, with targeted ransomware assaults on banks expected to increase in 2020, according to the report. A technique known as "JS Skimming," which employs malware to steal credit card information from E-Commerce sites such as Amazon's, is also on the rise. [183]

In August 2018, two men from Navi Mumbai were arrested for cyber crime. They were involved in fraudulent activities concerning money transfers from the bank accounts of numerous individuals by getting their SIM card information through illegal means. In July 2018, fraudsters hacked into Canara bank ATM servers and

[180] Rajan Sundaram 'Rise in Cyber Crimes – How Are Banks Fighting Back?' (2020) <https://www.jigsawacademy.com/rise-of-cyber-crimes-how-are-banks-fighting-back/ > accessed June 30, 2021

[181] ibid

[182] ibid

[183] ibid

wiped off almost 20 lakh rupees from different bank accounts. [184]The number of victims was over 50 and it was believed that they were holding the account details of more than 300 ATM users across India. The hackers used skimming devices on ATMs to steal the information of debit cardholders and made a minimum transaction of INR 10,000 and the maximum of INR 40,000 per account. On April 1, fraudsters conducted a cyber-attack against Cosmos Bank, a Pune-based bank, and stole INR 94.42 crores (USD 13.2 million). The dates are August 13 and 15, 2019.

Some of the systemic problems to cybersecurity in India, according to a recent research titled "Emerging trends and challenges in cyber security" by Reserve Bank Information Technology Private Limited (ReBIT), include the following:

- Lack of awareness.
- Budget constraint and low level support from higher management.
- Identity and access management are ineffective.
- Growing emergence of ransomware.
- Mobile device and apps.
- Attack of DDoS.
- Social Media

3.6 GROWTH IN CYBER CRIME DURING COVID-19 PANDEMIC

Financial institutions were in the forefront of the reaction to cyber risk during the covid-19 outbreak. The move toward greater working from home and other operational problems have increased their already high exposure to cyber risk. After the Covid-19 outbreak accelerated digitization and remote working, the financial sector is growing more vulnerable to cyber theft. Banks and other financial organizations are potential targets for cyber attackers because they hold valuable personal data and serve specific financial or economic requirements and sectors. Banks and other financial organizations are potential targets for cyber attackers because they hold valuable personal data and serve specific financial or economic requirements and sectors. Credit ratings can be harmed by cyber assaults mostly due to reputational damage and possibly monetary losses. Institutions with poor risk

[184] ibid

governance are less prepared for cyber assaults and thus more vulnerable.[185] Although learning from prior attacks and strengthening cyber-risk frameworks in real time is critical, the proper identification and response of attacks takes precedence because the nature of threats will continue to evolve.

Cyber risk is becoming more important as the economy and financial system become increasingly digitized. The phrase "cyber risk" refers to a wide range of dangers originating from the breakdown or breach of IT systems. Cyber risk is defined as "the combination of the possibility of cyber incidents occurring and their impact," according to the FSB Cyber Lexicon (2019). [186]In turn, a "cyber incident" is defined as "any observable occurrence in an information system" that:

(i) Jeopardizes the cyber security of an information system or the information it processes, stores, or transmits; or

(ii) Violates the security policies, security procedures, or acceptable use policies, whether or not as a result of malicious activity.

Aldasoro et al (2020b), CPMI-IOSCO (2016) define cyber risk as one type of operational risk. The cause/method, actor, intent, and effect of cyber hazards can all be categorised (Aldasoro et al (2020a), Curti et al (2019)).

The causes and tactics vary, and include both unintentional and deliberate attacks. Accidental data leakage, as well as implementation, setup, and processing failures, are examples of the former. Such occurrences are common. Yet, according to Aldasoro et al (2020c), around 40% of cyber incidents are deliberate and hostile, i.e., cyber attacks. [187]

Threat actors may inject themselves into a trustworthy data exchange in some cyber assaults. Malware (sometimes known as "malicious software") is software that is meant to harm computers and/or steal data (for example, so-called Trojans, spyware and ransomware). Attackers that inject themselves into a two-party transaction[188] (Graph 1, first panel), accessing or modifying data or transactions, are known as man-in-the-middle assaults.

[185] Inaki Aldasoro &Jon Frost & Leonardo Gambacorta & David Whyte, "Covid-19 and Financial Risk in the Financial Sector" (2021) 37 Bis Bulletin 3

[186] ibid

[187] ibid

[188] ibid

Cross-site scripting (XSS) is a web security flaw that allows attackers to hijack a victim's interactions with a vulnerable application. [189]

Working from home (WFH) has become more common as a result of Covid-19. To protect its employees, financial institutions, like other businesses, have temporarily shifted to remote working. As the majority of operations move to the digital realm, cyber attacks may become more common. In the first two months of the Covid-19 outbreak, for example, the use of remote access technologies such the remote desktop protocol and virtual private network (VPN) surged by 41% and 33%, respectively (ZDNet (2020)). If not properly managed, this could open up new chances for threat actors to breach IT systems and conduct cyber attacks, as well as other sorts of financial crime (Crisanto and Prenio (2020)).

Since covid-19 pandemic began, the banking industry has been hit by cyber attacks at a higher rate than the rest of the sectors. Advisen, a for-profit organization that collects information from credible and publically verifiable sources (primarily in the United States) covering date, actor, damage amount, and other attributes, can provide data about assaults. Between the end of February and June 2020, there is a substantial correlation between the prevalence of WFH arrangements – as evaluated by Dingel and Neiman's WFH index per industry – and the incidence of cyber attacks (Graph 2, left-hand panel). On both measures, the banking industry comes out on top. Outside of the health sector, the banking sector has had the highest number of Covid-19-related cyber events in recent months. Phishing attacks, for example, take advantage of the uncertainty surrounding Covid-19 to persuade users to open bogus attachments or give attackers access to networks.[190]

Payment companies, insurers, and credit unions have all been hit hard. The Financial Services Information Sharing and Analysis Center (FS-ISAC) conducted a survey of financial institutions and discovered a significant increase in phishing, suspicious scanning, and malicious activities against webpages used by WFH workers to access

[189] ibid

[190] "Rise in cyber crime post Covid is growing risk to bank ratings: S&P" Business Standard (India, 25 May 2021)

[191]the network. Payment businesses, insurance companies, and credit unions have seen the most hacking. With the spread of the pandemic, the number of Covid-19-related attacks increased from fewer than 5,000 per week in February to more than 200,000 per week in late April. In May and June, they increased by around a third compared to March and April (Check Point Research (2020)).[192]

Staff WFH swamped virtual desktop infrastructure (VDI)/VPN processes in 45 percent of situations, according to the survey. Business continuity IT plans were not created in one-third of cases for a long-term at-home workforce. During the pandemic, one-fifth of financial institutions stated that their network operations were disrupted.

So far, evidence reveals the same threat actors, intent, and methods as before the pandemic, but new opportunities due to the uncertainties around Covid-19. Phishing scams aren't new, but the number of people who fall for them has increased dramatically. According to a recent assessment, criminals and hostile nations used the Covid19 pandemic in a quarter of cyber incidents responded to in the United Kingdom between August 2019 and August 2020 (NCSC (2020)).

Threat actors infiltrated the European Union's (EU) VPN services, which allow employees to work from home (CERT-EU (2020)). [193]

Hackers have also attempted to break into the Indian State Tax Department's computers in order to obtain sensitive data such as PAN cards, GST numbers, phone numbers, and e-mail addresses. Hackers have attempted multiple efforts at banks and stock exchanges, all of which have resulted in the brokerage. The Hackers also targeted the COVID fund of Prime Minister David Cameron. [194]

Cyber-attacks have targeted not just local hospitals and testing institutes, but also the World Health Organization (WHO), stealing the passwords of WHO employees. Ransomware assaults have been discovered in hospitals and other testing facilities, where sensitive patient files are seized and not restored until a ransom is paid. Hospitals have been warned about ransom sites posing as government-approved

[191] ibid
[192] ibid
[193] ibid
[194] ibid

services to keep tabs on Corona patients, but which subsequently breach the system. [195]

3.7 CONCLUSION

The above discussion provides a brief summary of the current state of cybercrime in the banking industry, as well as the impact of cybercrime on bank finances. ATM frauds, Denial of Service attacks, Credit Card frauds, phishing, and other cyber crimes afflict the banking industry. The increasing growth of worldwide electronic crime, as well as the difficulty of investigating it, necessitates a global presence. The current precautions adopted by banks are insufficient, so it is critical to strengthen cooperation among banks throughout the world in order to develop tools and models that may be used to combat global financial cybercrime.

A cyber assault is predicted to affect one out of every four persons. Because of the high risk in this area, the financial sector must be constantly aware of the ever-increasing cyber threat. With the evolution of technology, many people have been kept in the dark about new technological breakthroughs, putting them exposed to cyber-attacks such as phishing and Trojans. There is no doubt about technological advancement in this field, as banking is one of the most sought-after sectors of the economy, and there will be constant updates to the software in use. The bank is responsible for ensuring that their client's data is secure and that the software in use is constantly updated.

The user should change their password every three months; nevertheless, banks are responsible for ensuring that their clients' data is kept secure and that the software they employ is kept up to date.

Every three months, the user should update their password; nevertheless, it is the responsibility of the bank to guarantee that the user is changing to a strong password. While a user is logging on, the bank should employ the concept of a trusted device to guarantee the user's identification. If a user attempts to log in using an unapproved device, the bank should send an SMS alert to the consumer to confirm. Finally, consumers must be aware of their credentials and ensure that they are not exploited. Banks must make special efforts to raise awareness and guarantee that clients do not

[195] ibid

become victims of scams. These measures have the potential to improve banking industry. .

As a result, it is reasonable to conclude that computer-related crime is a real and growing phenomena. Furthermore, a consistent increase in the frequency of such offenses in this area is projected, necessitating increased legislative attention.

CHAPTER 4

CYBER FRAUD IN BANKING INDUSRTY – LEGAL AND REGULATORY FRAMEWORK OF CYBER LAWS

4.1INTRODUCTION

The internet has now become an integral part of everyone's daily routine. It has taken over the world, from fundamental communications to internet purchasing. Companies have also chosen to carry on their operations via the internet. As a result, e-commerce has grown in popularity. Many government activities are now conducted online, and e-finance has exploded in popularity in the last year. As the internet has grown in popularity, so have the risks associated with it. Cyber law functions as a barrier in cyberspace, preventing cybercrime from taking place although it is a challenging task for legislators and law police. Officials have taken it upon themselves to draft and enact legislation to combat illegal online activity. Cyber law is a branch of law that deals with legal issues arising from the usage of interconnected information technology. In a nutshell, cyber law governs computers and the internet. [196]

The expansion of electronic commerce has prompted the need for more active and effective regulatory procedures to further enhance the legal infrastructure, which is so important to the success of electronic commerce. Cyber law encompasses all of these regulatory processes and legal infrastructures. Cyber laws are essential because they include practically all elements of transactions and activities that take place on or involve the internet, the World Wide Web, and cyberspace. Every online action and reply has certain legal and cyber law implications. Cyber law provides legal safeguards to those who use the Internet and conduct an online business. It is critical for Internet users to understand their country's local area and cyber legislation so that they can determine what acts are legal and which are not on the network. [197]They can also protect us from unlawful activity.

[196] Dr. Suresh V. Nadagoundar & M. P. Chandrika, "Law Relating to E-banking in India – An Outreach Challenge" (2018) 4 ISSN 117

[197] ibid

Intellectual property, contract, jurisdiction, data protection regulations, privacy, and freedom of expression are all covered by cyber law. It oversees the distribution of software, information, online security, and e-commerce via the internet. E-documents are given legal validity in the field of Cyber Law. It also establishes a framework for e-commerce and e-filling. To put it another way, the Cyber law is a legal framework for dealing with cyber offences. Due to the increased use of E-commerce, it is critical that suitable regulatory processes are in place to ensure that no malpractices occur.[198]

The law that governs cyberspace is known as cyber law. Computers, networks, software, data storage devices (such as hard disks, USB disks, and so on), the Internet, websites, emails, and even electronic gadgets such as cell phones, ATM machines, and so on are all included in cyber space. As previously said, cyber law is a discipline of law that deals with legal issues relating to the use of interconnected information technology.

In a nutshell, cyber law is the body of law that governs computer and internet offenses. Different countries have had different experiences when it comes to drafting and enforcing cyber legislation. Some early adopters in the United States and the West in general have enacted their own laws in this regard, either by adapting existing laws to the setting of cyberspace or by enacting new laws.[199]

In 1986, the Computer Fraud and Abuse Act (CFAA), was enacted. It was the first cyber law enacted by USA. Developing countries like as India, Pakistan, Indonesia, Malaysia, and the Philippines have passed cyber law legislation to follow in their footsteps. In general, there are numerous difficult legal challenges that law enforcement agencies from various countries have encountered and that have yet to be resolved. Cyberspace law legislators have encountered unique challenges in applying traditional legal principles to the setting of cyberspace.[200]

The National Policy on Information Technology 2012 was approved by the Union Cabinet in September 2012. The goal of the policy is to use information and communication technology (ICT) to address the country's economic and developmental issues. "To develop and deepen India's position as a global IT hub, and

[198] ibid
[199] ibid
[200] ibid

to leverage IT and cyber space as an engine for quick, inclusive, and substantial growth in the national economy," the policy's vision states.

4.1.1HISTORY OF CYBER LAWS IN INDIA

The Information Technology Act is the result of a resolution passed by the United Nations General Assembly on January 30, 1997, which adopted the Model Law on Electronic Commerce on International Trade Law.

This resolution recommended, among other things, that all states give the said Model Law careful consideration when revising or enacting new legislation, so that uniformity can be observed in the laws of the various cyber-nations governing alternatives to paper-based methods of communication and information storage.

The bill was written by the Department of Electronics (DoE) in July 1998.[201] However, it could only be introduced in the House on December 16, 1999 (after a nearly one-and-a-half-year hiatus) when the new Ministry of Information Technology was established. It was significantly altered, with the Commerce Ministry offering recommendations on e-commerce and problems relating to World Trade Organization (WTO) duties. This combined proposal was then vetted by the Ministry of Law and Company Affairs.

Following demands from Members, the bill was submitted to the 42-member Parliamentary Standing Committee after it was introduced in the House. The Standing Committee offered a number of recommendations that were included in the bill. Only suggestions that were authorized by the Ministry of Information Technology were taken into consideration. One suggestion that was hotly disputed was that a cyber caf6 owner keep a register with the names and addresses of all those who visited his caf6 as well as a list of the websites they visited. This idea was made in an effort to reduce cyber-crime and make it easier to track down a cyber-criminal. At the same time, it

[201] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 491

was mocked since it would infringe on a net surfer's privacy and would be unprofitable. [202]

Finally, the IT Ministry dropped this idea in the final draft. The bill was agreed by the Union Cabinet on May 13, 2000, and both chambers of the Indian Parliament enacted the Information Technology Bill on May 17, 2000. The President signed the bill on June 9, 2000, and it became known as the Information Technology Act of 2000.

The Act becomes effective on October 17, 2000.

With the advancement of technology and the emergence of new means of committing crime using the Internet and computers, the need to revise the IT Act, 2000 arose to include new types of cyber offenses and close other gaps that hampered the efficient implementation of the IT Act, 2000. As a result, the Information Technology (Amendment) Act, 2008 was passed and went into force on October 27, 2009. On various counts, the IT (Amendment) Act of 2008 has made significant revisions to the IT Act of 2000.[203]

4.1.2 NEED FOR CYBER LAW

Today's era is technologically advanced, the globe is becoming increasingly digitally sophisticated so are the crimes. Internet was created as a tool for study and information dissemination, and it was uncontrolled at the time. With e-business, e-commerce, e-governance, and e-procurement, it got more transactional over time. Cyber laws cover all legal issues relating to digital crime. As the number of people using the internet grows, so does the demand for cyber laws and their implementation. [204]

There are numerous security difficulties with utilizing the Internet, as well as various malicious people that attempt to get unauthorized access to your computer system in order to commit fraud. In the same way that any legislation is designed to protect online organizations and individuals on the network from unauthorized access and harmful people, cyber law is created to protect online companies and people on the

[202] ibid
[203] ibid
[204] Rajib Bhattacharyya, 'Information Technology and Cyber Law: A Globalized Review' (2018) 9 Indian JL & Just 115

network. If someone engages in illegal behavior or violates the cyber rule, it allows individuals or organizations to seek punishment or take action against them. [205]

In the present era, the world is highly digitized or computerized and the cyber law affects nearly everyone's life. For instance:

- Cyberspace is an ethereal dimension thus it is quiet difficult for the obsolete traditional law to govern and regulate it. Cyberspace needs its separate laws. That is why we need cyber laws which exclusively deal with cyberspace.
- There are no any jurisdictional boundaries in cyberspace. Within a couple of minutes, a person from India could break into a bank's electronic vault, which was hosted on a computer in the United States, and transfer millions of rupees to another bank in Switzerland. He'd only require a laptop computer and a cell phone. When a cyber fraud is done it is really difficult to identify from where the crime has been done. Therefore, to deal with jurisdictional issue cyber laws are important.[206]
- Cyber crimes are rising. Every second, cyberspace handles massive traffic volumes. Even as we read this, billions of emails are being sent around the world, millions of websites are being visited every minute, and banks are electronically transferring billions of dollars around the world every day.
- Any person can use cyberspace. There are no any terms and conditions applied to use and cyberspace. Without concern for the distance or anonymity between them, a 12 year old in Assam can have live chat session with a 10 year old in U.S.A.[207]
- Members of the cyberspace community have a lot of privacy and obscurity options. The security of information transmitted between cyber-citizens is ensured by readily available encryption software and steganographic tools that seamlessly disguise information within image and sound files.[208]
- Cyberspace provides unprecedented economic efficiency. Software worth billions of dollars can be traded over the Internet without the requirement for government licenses, shipping and handling fees, or customs duties.

[205] ibid
[206] ibid
[207] ibid
[208] ibid

- Cybercriminals have turned their attention to electronic data. It is characterized by extraordinary mobility, which outnumbers the mobility of people, products, and other services by a large margin.

  In a matter of seconds, international computer networks can send massive amounts of data throughout the world.
- A movie or a software source code which worth in crores of rupees can be pirated within hours of their release.
- Traditional penal provisions can only cover theft of physical information for instance, books, papers, CD ROMs and floppy disks but it is difficult for them to cover theft in cyber space. Only cyber laws which are exclusively for cyberspace can cover it.
- Nearly all transactions in shares are in demat form.
- Almost all businesses rely heavily on their computer networks and store sensitive information in electronic form.
- Government forms like income tax return, company law form etc. which used to be filled handwritten in paper form are now changed to electronic form which is to be filled electronically.
- Credit and debit cards gained its popularity among customers for shopping.
- The majority of people communicate via email, phone calls, whatsapp messages and text messages.
- The vital evidence of non-cyber crime such as murder, divorce, kidnapping, tax, evasion, organized crime, terrorist operations, counterfeit currency and so on are recorded computers and cell phones.
- Online banking fraud, online stock trading fraud, source code theft, credit card fraud, tax evasion, virus attack, cyber sabotage, phishing attacks, e-mails hijacking, pornography and other forms of cyber crime are becoming increasingly frequent.
- Obsolete transacting business is quickly replaced by e-signature and e-contracts.

4.1.3 POSITION OF CYBER LAWS IN INDIA

To begin with, India has a legal system that is exceedingly thorough and well-defined. The Constitution of India is the most important of the many laws that have been

enacted and executed. “The Indian Penal Code, the Indian Evidence Act of 1872, the Banker's Book Evidence Act of 1891, the Reserve Bank of India Act of 1934, the Companies Act,”and so on are just a few examples. The development of the Internet, on the other hand, signaled the emergence of new and complex legal challenges. It's worth noting that all of India's current laws were enacted long ago, taking into account the relevant political, social, economic, and cultural circumstances of the period. No one could imagine the Internet at that time. Despite our master draftsmen's remarkable foresight, the demands of cyberspace could never be predicted. As a result, along with tons of advantages the introduction of the Internet resulted in the formation of a slew of legal concerns and problems, necessitating the enactment of Cyber laws. [209]

Second, even with the most charitable and liberal reading, India's existing laws 16 could not be interpreted in light of the burgeoning cyberspace to embrace all aspects relating to various internet activities. In fact, actual experience and wisdom of judgment have revealed that interpreting existing laws in the context of evolving cyberspace without establishing new cyber laws will not be without serious risks and problems. As a result, relevant cyber laws must be enacted.[210]

Third, none of the existing laws offered cyberspace actions any legal validity or sanction. A huge majority of users, for example, use the Internet for email. Email is still not considered "legal" in our country. There is no law in the country that grants email legal status and consequence. In the lack of a formal statute approved by the Parliament, our courts and judges have been hesitant to provide judicial legitimacy to the legality of email. As a result, a need for Cyber law has evolved. [211]

Fourth, the Internet necessitates an up-to-date legal architecture that is both enabling and helpful. Because traditional laws have failed to provide this legal framework, only the passage of applicable Cyber laws can provide it. E-commerce, the Internet's most promising future, will only be conceivable if the required legal infrastructure is in

[209] ibid
[210] ibid
[211] ibid

place to support it. All of these factors, as well as a variety of others, contributed to the necessity for India to implement appropriate cyber laws.[212]

4.2 INDIAN STATUTES AND CYBER FRAUD IN INDIAN BANKING SECTOR

India is a member of the World Trade Organization (WTO).Liberalization, globalization, and privatization are the three core principles of the WTO.As a result, India's trade and commerce have been liberalized. In addition, the financial industry has seen significant changes. India is facing unprecedented competition from the rest of the world as a result of the introduction of e-banking. International trade would be a faraway dream if the financial sector's technology was not upgraded. The deregulation of the banking industry, combined with the emergence of new technology, has allowed new rivals to quickly and efficiently enter the financial services market. Various legal provisions that apply to traditional banking activities apply to internet banking as well. This does not solve the difficulties, hence more severe rules and laws aimed directly at e-banking issues are required.

In India, Internet Financial has become an important aspect of the banking system. In India the concept of e-banking is relatively new. Traditional banking, i.e. branch-based banking, was prominent until the early 1990s, when non-branch financial services were introduced. The Indian government passed the Information Technology Act of 2000, which took effect on October 17, 2000.A committee on Internet Banking was established by the RBI to look at various elements of Internet banking. The group concentrated on three important aspects of Internet banking: technology and security concerns, legal concerns, and regulatory and supervisory concerns. The RBI approved the working committee's observations and recommendations and gave guidance to banks on how to deploy online banking in India. Modern technology appears to be replacing the traditional manual techniques that have been prominent in Indian banking for millennia.[213]

[212] ibid

[213] [213] Dr. S. R. Myneni, Information Technology Law (Cyber Laws) (first published 2013, Rpt 2014 & 2016) 511

The RBI is in charge of banking, which is governed by the RBI Act. The Information Technology Act of 2000, as amended by the Information Technology Act of 2008, governs electronic reports. There are various legal frameworks that apply to traditional financial activities and also apply to e-banking. In any event, this does not address several concerns, necessitating the presentation of increasingly strict guidelines and guidelines especially to address e-banking issues. The Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934, and the Foreign Exchange Management Act, 1999, Indian Evidence Act, 1872, Indian Contract Act, 1872, Negotiable Instruments Act, 1881 as well as Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act (SARFAESI) Act, 2002 comprise the legal structure of the Indian financial framework. The Information Technology Act of 2000 attempted to solve a variety of internet business management challenges. However, there is a foggy condition that has not been adequately spelled out nor have any practical techniques of application been advocated by constitutional establishments.[214]

PROVISOINS UNDER IT ACT, 2000

Electronic commercial transactions and cybercrime are governed by the Information Technology (IT) Act of 2000, as modified in 2008. Negotiable documents, powers of attorney, trusts, wills and other testamentary dispositions, contracts for the sale of immovable property, and other transactions registered by the central government are all exempt from the Act's provisions. [215]

Section 1(2) read with section 75 – These two sections primarily concerned with privacy violations. The right to privacy may be included in the right to life and private liberty entrenched in Article 21 of the Indian Constitution. The many provisions of the IT Act 2000 effectively protect netizens' web privacy rights. The legal action that can be taken against the person who created the malware. Section 1(2) of the IT Act 2000, when read together with Section 75, allows for extraterritorial execution of the Act's

[214] ibid

[215] Rajib Bhattacharyya, 'Information Technology and Cyber Law: A Globalized Review' (2018) 9 Indian JL & Just 115

provisions. [216]As a result, if someone (including a foreign national) violates a person's privacy using an Indian computer, system, or network, he will be held accountable under the IT Act 2000.

Section 3(2) – This section deals with specific requirements for a specific technology as a means of authenticating records, such as bank servers and other virtual platforms via which banks supply us with E-Banking Services.

E-governance –In the chapter III, section 4 of Information Technology Amendment Act (ITAA), 2008 the legal recognition of electronic records is discussed in detail, followed by a description of procedures for electronic records, storage, and maintenance, and the recognition of the validity of contracts created using electronic means. Furthermore, any matter which shall be in writing or in a type-written form/printed form, shall be deemed to have been satisfied as true, notwithstanding anything contained in such law, if such information is rendered and certified in an electric form and is accessible so as to be usable for the subsequent reference.

Chapter IX of this Act deals with penalties, compensation and adjudication. These are the huge and important step towards tackle data theft, claiming damages, introducing security procedures etc which is discussed in section 43 of this Act.

Section 43 – Penalties and indemnification for computer and computer system and other property damage are dealt under section 43 of ITAA. Section 43 considers as the first crucial and substantial legislative move to tackle data theft in cyberspace. The Indian IT sector has argued and seeking for Indian legislation that deals with data theft in cyberspace for a long time. Data theft is a civil wrong that has been addressed under this section. If a person accesses or downloads, copies, or extracts any data from a computer without the permission of the owner or another person in charge of the computer, or introduces any computer contaminant such as a virus, or damages or disrupts a computer, or denies access to a computer to an authorized user, or tampers, he is liable to pay damages to the person so affected.[217]

This section is all about civil liability. Writing a virus software or sending a virus email, installing a bot, a Trojan, or any other malware in a computer network, or conducting a Denial of Service Attack on a server all fall under this section and will

[216] ibid
[217] ibid

result in civil liability. Computer Virus, Compute Contaminant, Computer Database, and Source Code are all described and defined in this section. The maximum damages under this heading were previously set at Rs.1crore in the ITA-2000, however this (the cap) was lifted in the ITAA 2008.[218]

Section 43A – The ITAA-2008 added Section 43A, which deals with damages for failure to protect data. This is yet another watershed moment in the field of data security, particularly at the corporate level. According to this Section, if a body corporate fails to adopt appropriate security practices and so causes unjust loss or gain to a person, the body corporate will be obliged to pay damages as compensation to the person affected. The section further clarifies the terms "body corporate" and "reasonable security methods and procedures," as well as "sensitive personal data or information."

Therefore, by adopting Section 43A, which requires corporations to ensure the implementation of appropriate security methods, the corporate responsibility for data protection is considerably highlighted. Furthermore, the federal government specified what constitutes sensitive personal data in its Notification of April 11, 2011, which included a list of all such data, including passwords, bank account or card details, medical records, and so on. Following this notification, the IT industry in the country, including tech-savvy and widely technology-based banking and other sectors, became acutely aware of the importance of data protection, and a general awareness of what data privacy is and what role top management and the Information Security Department in organizations play in ensuring data protection, particularly when handling sensitive data, grew.[219]

Section 65 – This section deals with tampering with source documents. Anyone who knowingly or intentionally conceals, destroys, or modifies any computer source code used for a computer, computer program, computer system, or computer network when it is required by law to be kept or maintained is guilty of a crime punishable by three years in prison or 2lakh rupees in fines, or both. The purpose of section 65 of the Act is to safeguard the "intellectual property" that has been invested in computer programs. It is an attempt to extend the protection provided by copyright laws to

[218] ibid
[219] ibid

computer source documents (codes). [220]Fabrication of an electronic record or forgery by interpolation in a CD produced as evidence in court (Bhim Sen Garg vs State of Rajasthan and others, 2006, Cri LJ, 3463, Raj 2411) are both punishable under this Section. In this section, "computer source code" refers to any listing of programs, computer commands, design and layout, and so forth.

Section 66 – This section deals with offenses involving computers. This section refers to the data theft mentioned in Section 43. Whereas in that section it was merely a civil offense with only compensation and damages as a remedy, here it is the same act but with a criminal intent, making it a criminal offense. If done dishonestly or fraudulently, the act of data theft or the offence described in Section 43 becomes a chargeable offence under this Section, which carries a sentence of up to three years in jail or a fine of up to 5lakh rupees, or both. Hacking was once defined as a crime under Section 66 of the Criminal Code.[221]

To be charged under section 66 of the IT Act, a person must cause a computer resource to perform a function with the dishonest or fraudulent intent to secure access, knowing that the access he seeks is illegal.

Section 66's essential components are:

1) Illegal access to a computer resource; and

2) “Fraudulent or dishonest motive

The violation of section 66 involves an infringement of a person's right and a reduction in the value or utility of that person's information stored on a computer resource. A computer-related offense entails a damaging mental act. The accused must cause the following: destruction, damage, disruption, denial, deletion, concealing, tampering, manipulation, stealing, or alteration of information contained in a computer resource owned, administered, used, or operated by any person (natural or legal).[222]

After the revision, data theft is now alluded to in Sec 66, making this section more meaningful and removing the term "hacking." The term "hacking" was once classified as a felony in this section, and courses on "ethical hacking" were also offered. As a

[220] ibid
[221] ibid
[222] ibid

result, people began to wonder how an illegal behavior could be taught academically with the word "ethical" appended to it. Then, for example, may there be training programs on "Ethical Burglary," "Ethical Assault," and so on for courses on physical defense? The ITAA resolved this thorny position by rewriting Section 66 to align it with Section 43's civil responsibility provisions and deleting the word "hacking." However, according to this Section, hacking is still a crime, even though some experts define "hacking" to mean "usually for good causes" (clearly to make labeling the courses "ethical hacking") and "cracking" to mean "for criminal objectives." It's worth noting that the technology used in both is the same, and the conduct is the same, however in "hacking," the owner's agreement is gained or assumed, and the latter act of "cracking" is considered a crime. [223]

Section 66B – Dishonestly receiving any stolen computer resource or communication equipment is punishable under Section 66B of the IT Act. The individual receiving the stolen property must have done so dishonestly or have reason to realize it was stolen property, according to this provision. Under Section 66B of the IT Act, this offense is punishable by imprisonment for up to 3 (three) years or a fine of up to Rs. 1lakh or both.[224]

Section 66C – Identity theft is punishable under Section 66C of the IT Act, which states that anyone who fraudulently or dishonestly uses another person's electronic signature, password, or other unique identification feature shall be punished with imprisonment of either description for a term that may extend to 3 (three) years, as well as a fine that may extend to Rs. 1lakh.[225]

Section 66D –As per section 66D of the IT Act "cheating by impersonation by using computer resource" as "any person who cheats by impersonation by using any communication device or computer resource," and states that any person who cheats by impersonation by using any communication device or computer resource shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to a fine which may extend to Rs. 1lakh.[226]

[223] ibid
[224] ibid
[225] ibid
[226] ibid

Section 69 – This is a fascinating section since it allows the government or specified agencies to intercept, monitor, or decrypt any information generated, sent, received, or stored in any computer resource, subject to the procedures outlined below. This power can be exercised if the Central Government or the State Government, as the case may be, believes it is necessary or expedient in the interests of India's sovereignty or integrity, defense, security, friendly relations with foreign states, or public order, or to prevent incitement to the commission of any cognizable offense relating to the foregoing, or to investigate a crime relating to the foregoing. In any such event, the required procedure must be followed, and the reasons for taking such action must be documented in writing by order directing any agency of the competent government. When requested, the subscriber or intermediary must provide all facilities and technical help.[227]

The ITAA was amended to include Section 69A, which gives the Central Government or any of its officers the authority to issue directives prohibiting public access to any information via any computer resource, under the same conditions as described above. The power to approve the monitoring and collection of traffic data or information through any computer resource is discussed in Section 69B.

Section 72 and 79 –These sections place responsibility for customer privacy breaches on the Service Delivering Agency or Intermediary, who is in charge of providing data services via their servers under particular terms and circumstances.

For the purpose of increasing the quality and condition of e-banking services on April 29, 2009, the G. Gopalkrishna Working Group (GCWG) produced a Report on the Security of E-Banking in India, with certain revisions, which now serves as the current regulatory requirements as an extension of IBG 2001.[228]

PROVISION UNDER THE INDIAN PENAL CODE, 1860

The Indian Penal Code (IPC) is a very powerful legislation that serves as India's fundamental criminal code. It is arguably the most commonly utilized in criminal jurisprudence. It encompasses practically all substantive aspects of criminal law and is supplemented by other criminal laws. [229]It was first enacted in 1860 and has been changed numerous times since then. Many special laws have been created in

[227] ibid
[228] ibid
[229] ibid

independent India having criminal and penal provisions that are frequently referred to and relied upon as an additional legal provision in circumstances where the relevant sections of the IPC are also referred to.

Indian Penal Code (IPC), 1860 does not define the term “cyber fraud” or “fraud”. The term "fraud" does not have a definition in the Indian Penal Code (In short, IPC). However, the IPC identifies and there are provisions for penalties of committing an act that may lead to the commission of fraud. Tomlin's Law Dictionary describes fraud as deception in land grants and conveyances, deals and sales of products, and other transactions to the detriment of another person, which may be accomplished by suppressing the truth or suggesting a falsehood. It means certain acts undertaken by a contracting party or his agent with the intent to deceive another party or convince him to enter into a contract, according to section 17 of the Indian Contract Act.[230]

The word "electronic" was added to the parts of the IPC dealing with records and documents by ITA 2000 with an amendment, thereby considering electronic records and documents on par with physical records and documents. Sections dealing with false entry in a record or false document (e.g., 192, 204, 463, 464, 468 to 470, 471, 474, 476, etc.) have since been amended as electronic record and electronic document, bringing all crimes involving an electronic record or electronic document within the ambit of the IPC, just like physical acts of forgery or falsification of physical records.[231]

Criminals who commit frauds in banking transactions may be prosecuted under the country's criminal legislation, which includes suitable punishment provisions under the Indian Penal Code, 1860.[232] In this regard, some of the most essential provisions of the IPC are discussed –

Section 383 – This section deals with punishment for extortion. Whoever knowingly and illegally makes a person believe that if they do not surrender any property or assets to him, he would slander them by posting some defamatory comment or article

[230] ibid
[231] ibid
[232] ibid

against them, will be penalized by imprisonment for up to three years, a fine, or both.[233]

Section 379 – This section deals with punishment for theft. Whoever unlawfully removes items or any electronic record from the hands of its legitimate owner without his express agreement will be penalized by imprisonment for up to three years or a fine, or both.

Section 403 – This section says that anybody who dishonestly misappropriates or converts any movable property to his or her personal use is punishable by imprisonment for a term up to two years, a fine, or both. For instance, A steals B's property in good faith, believing that it belongs to him. Misappropriation is not a crime committed by A. However, if A dishonestly misappropriates the property for his personal use after discovering his mistake, he is guilty of an infraction under this provision.

Section 405, 406 and 409 –As per the provision of section 405, anyone entrusted with property commits criminal breach of trust if he dishonestly misappropriates or converts the property to his own use, or if he dishonestly uses or disposes of the property in violation of any 3direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract he has made touching the discharging of such trust.[234]

Section 406 has provisions regarding the penalties for criminal breach of trust, which include up to three years in prison, a fine, or both. Criminal breach of trust by a governmental worker, a banker, merchant, or agent is punishable by up to ten years in jail under Section 409 of the IPC.[235]

Section 411 – Section 411 of the IPC, which is essentially equivalent to section 66B of the IT Act, also imposes penalties for dishonestly accepting stolen property. The penalty under section 411 of the IPC is either imprisonment of any kind for a period

[233] ibid
[234] ibid
[235] ibid

of up to 3 (three) years, or a fine, or both. Please note that the sole difference between the stipulated sanctions is that the IPC does not have a maximum fine cap.[236]

Section 415–As per the provision of this section, whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or who intentionally induces the person so deceived to do or omit to do anything that he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause, shall be punished.[237]

Section 417 – This section provides punishment for cheating. Whoever impersonates or willfully substitutes for another person and causes unlawful losses to an innocent victim shall be penalized by imprisonment for up to one year, a fine, or both.[238]

Section 463 – This section deals with forgery. Forgery is committed by anyone who creates a false document or electronic record, or a portion of a document or electronic record, with the intent to harm the public or any person, or to support any claim or title, or to cause any person to part with property, or to enter into an express or implied contract, or with the intent to commit fraud or that fraud may be committed.

Sections 354 D and 446 of the Indian Penal Code, as well as Sections 67A and 73-A of the Indian Evidence Act, 1872, have been changed by the IT Act. The Bankers Books Evidence Act, 1891, has been amended to embrace all electro-magnetic data storage devices, allowing all electronic data saved in such devices to be submitted as evidence in a court of law. Based on The Reserve Bank of India Act, 1934, it has also allowed the Reserve Bank of India's Central Board to control fund transfers using electronic means provided by banks or other financial organizations.[239]

Section 468 – As per this section, whoever commits forgery with the intent to use the falsified document for the purpose of defrauding is subject to imprisonment of either kind for a time that may extend to seven years, as well as a fine.[240]

---

[236] ibid
[237] ibid
[238] ibid
[239] ibid
[240] ibid

Section 469 – As per this section, whoever commits forgery with the intent that the forged document will harm the reputation of any party, or knowing that it will be used for that purpose, shall be punished with imprisonment of either description for a term that may extend to three years, as well as a fine.[241]

Section 471 – This section deals with using a genuine a forged document or an electronic record. Whoever fraudulently or dishonestly uses as genuine any document or electronic record that he knows to be forged faces a penalty of up to two years in prison or a fine, or both.

Section 500 – This section provides punishment for defamation. Whoever knowingly publishes any statement, image, or document on social platforms without any justification or reasonable cause, believing and knowing it to be false against any person, firm, or company where such imputation will definitely lower his image and intellect in front of the general public, shall be punished with simple imprisonment for up to two years or a fine, or both.[242]

Section 506 – This section provides punishments for criminal intimidation. A person who uses electronic means to threaten another person's reputation, life, or property in order to convince that person to conduct a criminal act or prevent him from doing something that is legally required of him is punishable by up to two years in prison, a fine, or both.[243]

PROVISIONS UNDER THE EVIDENCE ACT, 1872

The ITA has changed yet another piece of legislation. Prior to the enactment of the ITA, all evidence in a court was solely in tangible form. With the ITA recognizing all electronic records and papers, it was only reasonable that the country's evidence laws be updated to reflect this. The words "all documents, including electronic records" were substituted in the Act's definitions section. Words like "digital signature," "electronic form," "secure electronic record," and "information," as used in the ITA, were included to make them part of the evidential system in laws.[244]

[241] ibid
[242] ibid
[243] ibid
[244] ibid

Section 65B of this Act establishes the admissibility of electronic record. This is a lengthy part that serves as a watershed moment in the domain of evidence generated by a computer or electronic device. Any information contained in an electronic record printed on paper, stored, recorded, or copied in optical or magnetic media produced by a computer shall be treated as a document, without further proof or production of the original, if the following conditions are met: (a) the computer output containing the information was produced by the computer during the period over which the original was produced; (b) the computer output containing the information was produced by the computer during the period over which the original was produced; (c) the computer was in good working order for the most of the time period in question… and….a certificate signed by a person…responsible…etc.

To put it another way, evidences (information) obtained from computers or electronic storage devices and printed or stored on electronic media are valid if they were obtained from a system that was properly handled, with no room for data manipulation and ensuring data integrity, and accompanied by a certificate signed by a responsible person.

Nevertheless, one segment of the industry frequently misinterprets this section to indicate that computer printouts can be used as evidence and are valid as proper records even if they are not signed. Many computer generated letters from large corporations have a signature field below the words "Your faithfully" or "really," with the signature space left blank and a Post Script note at the bottom "This is a computer created letter and so does not require signature."The Act makes no mention of the fact that "computer print-outs do not need to be signed and can be used as a record."

PROVISIONS UNDER THE BANKERS' BOOK EVIDENCE ACT, 1891

The third schedule of the ITA contains amendments to this Act. Prior to the passage of the ITA, any evidence from a bank that was to be presented in court required the production of the original ledger or other register for verification, with the copy being kept in the court records as exhibits. 'Bankers' books' include ledgers, day-books, cash-books, account-books, and all other books used in the ordinary business of a bank, whether kept in the written form or as printouts of data stored in a floppy, disc, tape, or any other form of electro-magnetic data storage device," according to the ITA's definitions. When the books consist of printouts of data stored on a floppy, disc,

tape, or other medium, a printout of such entry...certified in accordance with the provisions....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in charge of computer system containing a brief description of the computer system and a brief description of the computer system by the principal accountant or branch manager.

In short, the provisions in the Bankers Books Evidence Act make a printout from a computer system, a floppy or disc, or a tape, a valid document and evidence, provided that such print-out is accompanied by a certificate stating that it is a true extract from the bank's official records and that such entries or records are from a computerized system with props.

Here again, let us reiterate that the law does not state that any computerized print-out even if not signed, constitutes a valid record. But still even many banks of repute (both public sector and private sector) often send out printed letters to customers with the space for signature at the bottom left blank after the line "Yours faithfully" etc and with a remark as Post Script reading: "This is a computer generated letter and hence does not require signature". Such interpretation is grossly misleading and sends a message to public that computer generated reports or letters need not be signed, which is never mentioned anywhere in nor is the import of the ITA or the BBE.

PROVISIONS UNDER OTHER LEGISLATIONS

Income Tax Act, 1961 – Section 40A (3) of this Act deals with e-banking. This section's benefit is only available to the account holder if the money is transferred via internet banking or a check. This clause aims to prevent tax avoidance by requiring all transactions over $20,000 to be reviewed by the bank.[245]

Negotiable Instruments Act, 1981 – Under Section 6 of this Act the Truncated Cheque and e-cheque concepts were added. These cheques are electronic negotiable instruments that are part of online banking. With the use of digital signatures, all of these instruments are needed to meet minimal security requirements (which may be linked with biometric).[246]

[245] ibid
[246] ibid

Prevention of Money Laundering Act, 2002 – Section 11 imposes duty on every financial institution and intermediary. Every financial institution and intermediary is required to keep a record of every transaction.[247]

This is true for all banks, whether they provide physical or online services. This provision aids in the prevention of money laundering via the internet banking system.

Consumer Protection Act, 1986 – The purpose of this act is to safeguard the interests of consumers.

It can also be applied to banking services. This act protects problems including privacy, the confidentiality of consumer accounts, and the rights and duties of customers and banks in relation to internet banking.

4.3 ROLE OF RBI IN E-BANKING AND CURBING CYBER FRAUD

The RBI, as the central bank and ultimate regulator of the Indian banking industry, has detailed policy rules and procedures for detecting, investigating, and prosecuting various sorts of bank frauds, as well as preventing and reporting them. It is public knowledge that banks do not follow the central bank's recommendations in most cases of fraud. The central bank, as part of its routine, takes a number of proactive actions to combat bank fraud.[248]

RBI and the GOI have enacted a number of legal and regulatory rules that govern banking in India. The RBI provides circulars and instructions on numerous elements of banking on a regular basis. The rules may differ based on the type of bank, such as a Scheduled Commercial Bank, a Non-Bank Financial Corporation, a Regional Rural Bank, or an Authorized Dealer Bank. The RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds, which were released in April 2011, outline the basic information security rules that all banks must adhere to.[249]

RBI plays a crucial role in giving identification to e-banking in India. To ease electronic fund transfers and assure the legal admissibility of documents and records, transactions such as Real Time Gross Settlement (RTGS), National Electronic Fund

[247] ibid

[248] Nilotpal Dev Roy. 'E-banking Frauds and Indian Legal Perspective' (2020) <https://www.legalserviceindia.com/legal/article-3322-e-banking-frauds-and-indian-legal-prospective.html > accessed July 10 2021

[249] ibid

Transfer (NEFT), and other kinds of fund transfer are used. The Reserve Bank of India uses the electronic payment systems Electronic Cleaning Service (ECS) and Electronic Fund Transfer (EFT), both of which were implemented in 1995, as well as the RTGS system in 2004, the NEFT system in 2005, and the cheque transaction system in 2008.[250]

RBI also provided instructions on card present transaction security and risk reduction measures. In this circular, the RBI has taken steps to secure card-not-present transactions by requiring banks to implement extra authentication or validation for any recurring transactions involving information not available on credit, debit, or prepaid cards.

The RBI also instructed banks and other stakeholders to take immediate measures to complete the following tasks in a timely manner. It also regulates the application of fraud risk management techniques and the security of India's digital infrastructure for commercial banks. With the Banking Laws Amendment Act of 2012, the RBI now has the authority to request any information and inspect the business of any of the bank's partner enterprises.

It also established the legal basis for the formation of bank holding corporations and paved the path for the licensing of new banks. The Reserve Bank of India (RBI) has issued numerous rules and regulations to commercial banks in the areas of information technology, electronic banking, and technological risk.[251]

In India, electronic banking transactions have grown at an unprecedented rate, especially since the government announced demonetization in November 2016.Mobile banking, debit cards, and credit card transaction quantities have all increased by 200 percent, 165 percent, and 45 percent year over year, according to reports. This surge in e-banking transactions has coincided with an increase in unlawful or fraudulent activities.[252]

Banks were required to pay customers if they were at fault under previous RBI restrictions on fraudulent transactions. Banks were expected to pay customers for third-party errors in accordance with their customer relations policies. Nevertheless,

[250] ibid
[251] ibid
[252] ibid

these RBI regulations did not specify the scope of obligation or the timelines for compensation, and client claims were often rewarded after the banks' insurance claims were resolved.[253]

The RBI Circular directs banks to improve their systems and procedures in order to maintain the security of electronic banking transactions. Having a robust and dynamic fraud detection and prevention mechanism, a system to assess the risk of illegal transactions and associated liabilities, methods to mitigate the risks and assure liability protection, and consumer awareness are just a few of them.

The RBI Circular also mandates that banks provide a method for compensating customers in the event of fraudulent transactions in their customer relations policies. They must also set up a method to notify their board of directors or board committees of any occurrences of customer liability.[254]

4.3.1 RBI CIRCULAR TO CONTROL RISK DUE TO E-BANKING

The RBI has issued a new E-Banking Circular. As a supervisor, the Reserve Bank of India would cover all risks related with electronic banking as part of its normal responsibilities. Every bank has a legal obligation to draft a clear Customer Acceptance Policy that lays out the criteria for customer acceptance. The Customer Acceptance Policy must include explicit rules for the following components of the bank's customer relationship.[255]

- No account should be created under a false or fictitious name. Banks should not allow or maintain anonymous accounts or accounts in false names or accounts on behalf of other people whose identities have not been revealed or cannot be verified.
- Risk perception parameters are clearly specified in terms of the kind of business activity, customer and client location, mode of payment, volume of turnover, social and financial standing, and so on, allowing consumers to be

[253] ibid
[254] ibid
[255] Dr. Suresh V. Nadagoundar & M. P. Chandrika, "Law Relating to E-banking in India – An Outreach Challenge" (2018) 4 ISSN 117

classified as low, medium, or high risk. Customers who require a high level of monitoring may be classified even higher if it is deemed necessary.[256]

- Banks can only effectively regulate and decrease risk if they have a thorough awareness of their customers' usual and reasonable activities, as well as the tools to spot transactions that deviate from that pattern. The level of monitoring, however, will be determined by the account's risk sensitivity.

  All complex, exceptionally big transactions, as well as all strange patterns with no clear economic or visible legal reason, should be scrutinized by banks. Banks may set threshold limitations for a certain type of accounts and pay special attention to transactions that exceed such limits. A transaction requires substantial sums of money that is not consistent with the customer's typical and expected behavior should draw the bank's notice. Account turnover that is out of proportion to the size of the balance held could suggest that monies are being 'washed' through the account. Accounts with a high risk level must be closely monitored. Every bank should establish key indicators for such accounts, taking into account the customer's background, such as the country of origin, funding sources, transaction types, and other risk characteristics. Banks should consider the high risk associated with accounts of bullion dealers (including sub-dealers) and jewelers when identifying suspicious transactions and filing Suspicious Transaction Reports (STRs) with the Financial Intelligence Unit-India (FIU-IND)Banks should establish a mechanism for reviewing account risk categorization and the requirement for heightened due diligence steps on a regular basis. This review of client risk categorization should be done at least once every six months.[257]
- Banks are required to monitor the accounts of Multi-Level Marketing (MLM) companies that entice public funds with the promise of big profits. They send interest and principal money in the form of post-dated checks. The chain breaks and the cheques are dishonored once public deposits halt. As a result, banks should investigate suspicious transactions in accounts when a significant number of cheques with similar dates/amounts are issued. The RBI

[256] ibid
[257] ibid

and the Financial Intelligence Unit India should be informed about the situation.[258]

- Internal audit and compliance activities of banks play a critical role in assessing and assuring compliance with KYC policies and processes. In general, the compliance function should provide an impartial assessment of the bank's policies and procedures, as well as legal and regulatory obligations. Banks should ensure that their auditing departments are fully staffed with people who are familiar with such policies and processes. Concurrent/Internal Auditors shall inspect and verify the application of KYC procedures at the branches, and comment on any lapses that are discovered. Compliance in this area should be presented to the Board's Audit Committee on a quarterly basis.[259]
- Banks should pay close attention to any potential money laundering dangers posed by new or evolving technologies, such as online banking, which may favor anonymity, and take steps to prevent their use in money laundering schemes if necessary. Many banks issue a variety of electronic cards that users use to buy goods and services, withdraw cash from ATMs, and send money electronically.

  Banks must ensure that any KYC/AML/CFT rules released from time to time are followed in full, including for add-on/supplementary cardholders. Furthermore, credit card marketing is typically done through the use of agents. Before providing cards to customers, banks should guarantee that proper KYC procedures are followed. It's also a good idea for agents to be submitted to KYC procedures.[260]
- Wire transfer is the fastest and most convenient way to send money over the world. As a result, it is necessary to prohibit terrorists and other criminals from having unrestricted access to wire transfers in order to move their funds and to discover their misuse. This can be accomplished if basic information on the originator of wire transfers is made promptly available to appropriate law enforcement and/or prosecution authorities to aid them in discovering, investigating, prosecuting, and tracing terrorists or other criminals' assets.

[258] ibid
[259] ibid
[260] ibid

[261]Financial Intelligence Unit - India (FIU-IND) can use the data to investigate suspicious or anomalous activities and disseminate it. The beneficiary bank can also use the originator information to aid in the identification and reporting of suspicious transactions to FIU-IND. Because minor wire transfers may constitute a threat to terrorist financing, the goal is to be able to track all wire transfers with minimal threshold constraints.[262] As a result, banks must guarantee that all wire transfers include the following details:-

a) The originating information for all cross-border wire transaction must be accurate and meaningful.
b) The name and address of the originator, as well as the account number if one exists, must be included in the information accompanying cross-border wire transfers.
c) When several individual transfers from a single originator are bundled together in a batch file for transmission to beneficiaries in another country, they may be exempt from including full originator information if they include the originator's account number or unique reference number.

- Banks are mandated to keep transaction records and notify the Financial Intelligence Unit India whenever a suspicion develops. Banking firms are required to keep and submit client account information to the Financial Intelligence Unit India, and they should take all necessary steps to maintain compliance.[263]
- The nature of the transactions; the amount of the transaction and the currency in which it was denominated; the date on which the transaction was conducted; and the parties to the transaction are all required to maintain and preserve all necessary information in respect of the transactions referred to and to permit the reconstruction of individual transactions.[264]
- All suspicious transactions should be reported to the RBI.

[261] ibid
[262] ibid
[263] ibid
[264] ibid

All banks have been instructed by the RBI to accept the circular in spirit and letter, and if they are unable to do so, to submit a "nil" report.

4.3.2 RBI'S NEW GUIDELINES FOR CUSTOMERS AGAINST ANY ONLINE FRAUD

The Reserve Bank of India has devised the concepts of "zero liability" and "limited liability," which make electronic payments safer for bank clients. Customers will not suffer any losses under the new program if illicit electronic banking transactions are notified within three days and the funds are credited to the account within ten days. The RBI's circular applies to both online and in-store transactions involving electronic payments.[265]

The following are the final rules aimed at ensuring the safety of online transactions.

- In the event of a third-party breach or the bank's negligence, the customer will have no liability. If an unlawful transaction is reported to the bank within three working days, the customer will not be held accountable.
- When a customer's negligence causes a loss, such as revealing a password, the customer is responsible for the entire loss until he notifies the unlawful transaction to the bank.
- Within 10 working days after the customer's notification, the bank must credit the amount involved in the improper electronic transaction to the customer's account.
- If a consumer reports a fraudulent transaction within four to seven working days, the maximum liability ranges from Rs. 5,000 to Rs. 25000, depending on the kind of account.
- If a fraud is reported within seven working days, the customer will be held liable according to the bank's policy.
- Internet banking and mobile banking, as well as ATM and point-of-sale transactions, are all included in the transactions.
- The banks must include a direct link to file complaints on their home page of their website.

[265] Jaro Jasmine & Aswathy Ranjan, "A Critical Study on Concept of E-Banking and Various Challenges of IT in India with Special Reference to RBI's Role in Safe Banking Prsctices" (2018) 119 Int'l J Pure Applied Math 1661

- RBI has ordered banks to require their clients to sign up for SMS and email alerts. Customers must be able to respond to such alerts with a Reply option so that banks can be notified quickly in the event of fraudulent transactions.[266]

4.4 JURISDICTIONAL ISSUES IN CYBER SPACE

Jurisdiction refers to a court's ability to hear and decide on a case so that they can adjudicate and exercise any judicial power over it. Thus, jurisdiction refers to the court's authority to decide on topics that are disputed before it or to take notice of items that are brought to it in a formal manner for its determination.[267]

Commonly, there are two types of jurisdictions:

1. The court's subject jurisdiction permits it to decide cases of a specific type and determine whether the claim is actionable in the court where the case was filed.
2. Personal jurisdiction empowers a court to rule on issues involving citizens or residents of its territory who have a relationship to that territory, regardless of where they are now located. Every state has personal jurisdiction over the persons who live inside its borders.

Jurisdictional issue in cyber crime is the most crucial problem. For instance, in the matter of seconds, a person in Pakistan could get into an Indian bank's host computer and transfer billions of rupees to a bank in China.[268]

He'd only need a computer system, mobile phone and internet to complete this crime. When a crime is committed, there is a question of jurisdiction as to where the complaint should be filed for trial. This is due to the fact that different countries' rules on how to deal with cybercrime situations differ.[269]

Jurisdiction simply refers to the concept of a legal system's competent Court having the authority to decide and hear a matter. The fact that parties interested in a dispute are essentially positioned in separate regions of the world and have only a virtual

[266] ibid
[267] Dr. Adel Azzam Saqf Al Hait, "Jurisdiction in Cyber Crimes: A Comparative Study" (2014) 22 JL Pol'y G11N 75
[268] ibid
[269] ibid

connection that binds them all into one realm is the fundamental issue that clouds Cyber Space Jurisdiction. Although the internet has blurred geographical and jurisdictional lines, internet users continue to be subject to laws that are independent of their presence on the internet.[270]

A single online transaction may be governed by the laws of the user's home state, the laws of the state where the transaction server is situated, or the laws of the state where the person with whom the transaction is conducted. As an example, if a person in the United States conducted a transaction with another user in Indonesia via a server in Chennai and had problems, they would theoretically be subject to the laws of all three nations involved.[271]

Normally, the jurisdiction is determined by the location of the cause of action. When there are several parties participating in different parts of the world, however, determining jurisdiction becomes extremely complex. In the cyberspace, a transaction essentially involves three participants. The user, the server host, and the person with whom the transaction is being conducted must all be placed under the same jurisdiction.[272]

When the contractual parties or the parties in dispute are of different nationalities, matters of jurisdiction become a matter of state and international law. When there are international parties to a dispute, the State is subjected to the application of its legislation under international law.[273]

4.4.1 JURISDICTION OVER CYBER CRIME AND INDIAN LAWS

When it comes to determining jurisdiction in the context of cyberspace, it becomes a difficult part of law. Jurisdiction is the power or authority of the court to hear and determine the cause and adjudicate upon the matter that is litigated before it, or the power of the court to take cognizance of the matter brought before it.[274]

India, in general, is not yet fully adaptive to new technology and thus, doesn't consider the same as a fit mechanism to undertake any legal obligations. As a consequence of the same, only a certain handful of cases concerning personal Cyber

[270] ibid
[271] ibid
[272] ibid
[273] ibid
[274] ibid

Space Jurisdiction have been decided by superior courts in India.[275] The approach adopted here is very similar to the minimum contacts approach used in the USA. The exercise of jurisdiction is regulated by procedural laws.
For all questions of civil law, the Civil Procedure Code, 1908 governs jurisdiction under Indian law. Pecuniary jurisdiction is provided by Section 6 of the Act, while subject matter jurisdiction is provided by Section 16.In addition, Section 19 deals with cases involving movable property, whereas Section 20 specifies the location of the defendant or the cause of action, i.e. territorial jurisdiction.[276]

Section 20 provides essential elements for the initiation of an additional suit in a court within the local limits of whose jurisdiction;

- The defendant or each of the defendants resides, conducts business, or individually works for profit at the time the suit is filed,
- Any of the defendants, where there are more than one defendants, resides, carries on business, or personally works for gain at the time of the commencement of the suit, provided that either the court grants leave, or the defendants who do not reside, carry on business, or personally works for gain, as aforesaid, acquiesce in such institution or,
- The cause of action wholly or paternally.

This section, however, does not appear to be appropriate in the virtual world. The issue with Section 20 is that, while it provides for geographical jurisdiction, it does not account for parties who are located in separate jurisdictions but communicate through a different medium. The problem with cyberspace jurisdiction is that it involves multiple parties from all over the world who only communicate via virtual connections. As a result, we can't get a clear picture of the parties and the location of the lawsuit so that the court's jurisdiction to hear such cases can be determined.[277]

The Information Technology Act, 2000 (IT Act), which went into effect on October 17, 2000, is the main source of cyber legislation in India. The Act's goal is to provide e-commerce legal legitimacy and make it easier for the government to store electronic information. The IT Act also penalizes and punishes numerous forms of cybercrime.

[275] ibid
[276] ibid
[277] ibid

[278]There are several provisions in this legislation that render the idea of judicial jurisdiction for the trial of cases involving cyber crimes in India as well as beyond India.

Though the ITA was significant first step and a watershed moment in the nation's technological development, the existing legislation is insufficient. Many concerns and crimes involving cybercrime remain unsolved.

Territorial Jurisdiction is a major issue that the ITA does not adequately address. Jurisdiction is addressed in Sections 46, 48, 57, and 61 in connection with the adjudication process and the appellate procedure, and again in Section 80 as part of the police officers' powers to enter and search a public place for a cyber crime, among other things. Because cyber crimes are mostly computer-based offenses, determining which P.S. will take cognizance is challenging. For example, if someone's email is hacked in one location by an accused sitting in another state, determining which P.S. will take cognizance is tough. On the whole, it appears that investigators try to avoid accepting such accusations on the basis of jurisdiction. Because cybercrime is geographically agnostic, international, territory-free, and frequently dispersed across multiple jurisdictions, it is necessary to provide proper training to all involved participants in the field.

Preservation of evidence is also big issue. It is obvious that while filing cases under IT Act, very often, chances to destroy the necessary easily as evidences may lie in some system like the intermediaries' computers or sometimes in the opponent's computer system too.

Nevertheless, the majority of cyber crimes in the country are still prosecuted under the relevant sections of the IPC in conjunction with the comparative sections of the ITA, giving investigating agencies the assurance that even if the ITA part of the case is lost, the accused cannot escape the IPC part.

4.4.2 JURISDICTIONAL OVER CYBER CRIMES AND INTERNATIONAL CONVENTIONS

The United Nations Convention on Transnational Organized Crime (UNTOC) was adopted by the General Assembly on November 15, 2000. It is currently the UN's

[278] ibid

major international convention dealing with transnational organized crime. It is a symbol of the UN's commitment to combating transnational organized crime.[279]

Though there is no specific definition of cybercrime under UNTOC, however cybercrime can be encompassed by its articles when internet is utilized as a venue for committing organized crime. On the one hand, organized criminal groups are intrinsically linked to cybercrime. There is evidence that sophisticated criminal organizations have exploited internet technology to commit crimes such as online pornography, hacking, money laundering, fraud, and theft.[280]

Cybercrime, on the other hand, is a global phenomenon. According to Section 3 of the UNTOC, an offense is transnational if:

(a) It is committed in more than one State;

(b) It is committed in one State but a substantial part of its preparation, planning, direction, or control takes place in another State;

(c) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or

(d) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one (Section 3, United Nations Convention on Transnational Organized Crime).

Computer crimes can be committed by a criminal in one jurisdiction against a victim in another country in the cyber world. This crime can take place in multiple nations at the same time. Similarly, cybercriminals can quickly change their location from one country to another to avoid identification and arrest.[281]

The UNTOC can be used as a basis for enacting steps to gain jurisdiction over different computer-related offenses, given the global character of cybercrime and its relationship with organized criminal groups.[282]

The grounds by which the contracting parties to the convention may gain jurisdiction over the offenses covered by UNTOC are laid out in Article 15 of the agreement.

It stipulates that when a crime covered by the convention is committed within a contracting party's territory, the contracting party may establish jurisdiction over the offence. This is a restatement of the criminal law's Territorial Principle, which holds that all crimes committed within a country's territory are subject to its jurisdiction.

[279] Miss Prevy Parekh & Miss Tarunya rao, “Cyber Space and Jurisdiction” (2018) 2 JCIL 1
[280] ibid
[281] ibid
[282] ibid

[283]When a computer-related crime is committed on board a vessel or inside an aircraft that is registered under the laws of the country, jurisdiction may be established. This is because ships and planes are regarded extensions of a country's territory.

When the victim or perpetrator of a computer-related crime is a national of one of the UNTOC's contracting parties, jurisdiction over the offense may be established. This is in line with the notion of active personality.[284]

As a result, even if the crime takes place in a different country, if the victim is a citizen of that nation, the latter government may still have jurisdiction over the cybercrime. A contracting party to the UNTOC may also acquire jurisdiction if a stateless person who habitually resides in the territory of one of the signatories to the UNTOC commits a cybercrime. This is in line with the notion of passive personality.

Under Article 5 part 1, a contracting party may acquire jurisdiction over cybercrime even if the crime is committed outside its territory if the perpetrators of the crime intend to commit a severe crime within its territory. Thus, under the UNTOC, a contracting party can exercise jurisdiction over a person who organizes, directs, aids, abets, or facilitates the commission of cybercrime involving an organized crime even if the crime is committed outside the territory, as long as the intention to commit the crime within the territory can be established.

When a crime is committed inside the territory of a contracting party by a person who is a national of another country, Article 15 part 3 establishes a hierarchy in the claims of jurisdiction in respect to Article 16 paragraph 10. When the contractual country whose national committed the crime does not opt to extradite its national in favor of another contracting party, the latter is required by the agreement to prosecute its nationals. [285]

The treaty specified that when a national is prosecuted for a crime committed outside of its territory, the perpetrator will be treated as if he or she had committed a serious crime. Other states are likewise required by the convention to cooperate in the filing of evidence against the culprit.[286]

Article 15 part 4 states, on the other hand, that if the perpetrator of the crime is present within the territory of one of the contracting parties and the crime was

[283] ibid
[284] ibid
[285] ibid
[286] ibid

committed against another contracting party, the former is obligated to assume jurisdiction over the crime for the purposes of prosecution.

On the problem of multiple jurisdictions over the same offense committed against various countries, Article 15 part 5 follows the case-by-case deliberation procedure. If a cybercrime is perpetrated against multiple contracting parties, the parties are required to coordinate and consult with one another. The goal is to guarantee that the actions are coordinated and that the prosecution is successful.[287]

4.5 CONCLUSION

It's reasonable to conclude that computer-related crime is a serious and growing problem. Furthermore, a consistent increase in the frequency of such offenses in this area is projected, necessitating increased legislative attention. The current conceptual framework has provided a bird's eye view of ongoing efforts to prevent and manage high-tech and computer-based crimes, as well as emphasizing broad trends and developments within and outside the Indian banking sector. Cybercrime knows no bounds and evolves at the same rate as new technologies. Cybercrime's enormous expansion and tragic repercussions pose a serious danger to banking and financial institutions. Its goal is to create robust security preparedness among financial institutions, such as banks. The growing reliance on electronic banking technology by billions poses a significant challenge for cyber professionals in developing a reliable cyber security procedure.

In order to combat cyber weaknesses, Indian banks must also combat their attitudes and be psychologically prepared to cope with cybercrime and criminals on a war footing. The entire Orthodox procedure should be abandoned, and new technologies with an agile and radical combat system should be implemented. A study of the cyber security landscape and upcoming risks is also required.

Banks are considers as the country's financial backbone and a tool in the hands of individuals and institutions. At no cost, a healthy banking institution / bank's trustworthiness should be jeopardized. Now is the time for banks to break free from

[287] ibid

their old banking frameworks and collaborate with new technologies and a fresh perspective in order to eliminate or reduce the cyber threat in the system.

CHAPTER 5

JUDICIAL PRONOUNCEMENTS ON CYBER FRAUD IN BANKING SECTOR

5.1INTRODUCTION

There has been a tremendous growth in cyber scams around the world as the use of digital technologies has increased significantly over the years. The sophistication of cyber criminals has increased, making it increasingly difficult for businesses to defend themselves against cyber attacks. We now rely even more heavily on the internet as technology improves. Work, leisure, shopping, and banking are all things that can be done online. Daily tasks have become significantly easier thanks to the internet. Nevertheless, it has resulted in a significant increase in cybercrime all across the world. Due to the rising use of internet banking by Indians, the number of online banking frauds in India has increased significantly.

According to the RBI's annual report, "bank frauds involving 100,000 or more people rose to 1.855lakh crores in FY20, up from 71,500crores in FY19."[288]

In the same time span, the number of such cases has climbed by 28%.The banking sector, on the other hand, has been making persistent attempts to secure its systems and users. Malicious actors, on the other hand, use numerous methods to deceive individuals on the internet in order to steal their money or sensitive information.[289]

From April 2009 to September 2019, India lost a total of 615.39crores in more than 1.17lakh cases of online banking fraud, according to a Hindustan Times article. These frauds have occurred during a ten-year period. Nevertheless, the frequency of online banking frauds is on the rise in the banking business. There was a concentration of high-value crimes, with the top 50 credit-related frauds accounting for 76 percent of all frauds registered in 2019-20. Other banking-related incidents, like as off-balance sheet and foreign transactions, decreased in 2019-20, according to the RBI.[290]

---

[288] Richard Singha, 'The Rising Online Banking fraud in India' (2021) < https://www.google.com/amp/s/securityboulevard.com/2021/01/the-rising-online-banking-frauds-in-india/amp/?espv=1 > accessed July 20 2021

[289] ibid

[290] ibid

In the previous three months of 2019, 129crores were stolen, with a total of 21,041 such cases being registered," stated Anurag Thakur, MoS, Ministry of Finance, in the Lok Sabha, referring to a recent internet fraud in India.

5.2CASE STUDY ON CYBER ATTACKS IN INDIAN BANKING INDUSTRY

1. Official website of Maharashtra Government (Hacked Mumbai): IT experts attempted to reclaim control of the Maharashtra government's hacked official website on September 20, 2007. The website http://www.maharashtragovernment.in remained unavailable. The Maharashtra government website has been hacked, according to Vice President Pastor and Home Priest R.R Patil. He promised that the state government will investigate the hacking and instructed the Digital Wrongdoing Branch to look into it. Patil stated that if necessary, the state would recruit private IT experts in this area.[291]

The Middle Easterner News learned that programmers may have obliterated the majority of the site's content while re-establishing the site. The hackers were identified as Program Cool Al-Jazeera, according to IT officials, and they were based in Saudi Arabia. The official site has been influenced by malware on a few occasions before, but has never been hacked, according to a senior government IT officer.[292]

People were misused through internet techniques for booking air tickets, and three people were held accountable for the on-line Visa scam. The Digital Wrongdoing Examination Cell in Pune aided these parties. Mr. Parvesh Chauhan, an extra security officer with ICICI Prudential, gripped one of his clients. According to information provided by the police, one of the clients received a notification for purchasing airline tickets while his master card was in his possession. When he learned of the problem, he went straight to the bank. The tickets were purchased via online methods.[293]

After further investigation, it was discovered that the data was obtained from the State Bank of India. Shaikh worked in the Visa department and had access to the new client

[291] Harshita Singh Rao, "Cyber Crime in Banking Sector" (2019) 7 Int'l J Res Granthalaya 148
[292] ibid
[293] ibid

information. He also told Kale about the information. Kale then passed this information on to his friend Lukkad, who used the information to book air tickets and sell them for the same amount of money. DCP Sunil Pulhari, the head of the Digital Cell, was involved for eight days before catching the criminals.[294]

2. UTI bank hooked in a phishing attack: In February 2017, a phishing attempt on UTI bank's website resulted in the bank being caught in a phishing campaign. A geo cities URL was sent to the client's email addresses, requesting personal details such as login Id and password. The web page not only requests account information such as user and transaction credentials and passwords, but it also includes deceptive disclaimers and security risk statements. IT officials eventually learned that the page's website admin was a man named PetrStastny, whose email address could be seen on the page. The Monetary Office Wing of the Delhi Police has been alerted about the case, according to top UTI bank officials. The bank has also enlisted the help of Melbourne-based Extortion Watch Worldwide, a leading organization that monitors phishing and works to prevent it.[295]

The bank has also enlisted the help of Fraud Watch International, a premier anti-phishing firm based in Melbourne that provides phishing monitoring and take-down services. V K Ramani, President of IT (UTI Bank), said that they are now in the process of shutting down the website. Some of these projects require time, but clients have been kept informed about them, said V K Ramani.[296]

According to the findings of UTI Bank's security department, phishers have sent over 1,00,000 emails to UTI Bank and other bank account users. Despite the fact that the corporation has begun damage control efforts, none of them are completely foolproof.

According to Ramani, banks now have no means of knowing if the individual coming in with legitimate user credentials is a fraud. However, trustworthy sources within the

[294] ibid
[295] ibid
[296] ibid

bank and security agencies confirmed that the bank and security agencies suffered no losses as a result of this attack. In addition to beefing up its warning and fraud response system, the bank has sent out alerts to all of its customers informing them about such harmful websites. According to Sanjay Haswar, Assistant Vice President, Network and Security, UTI Bank, using professional businesses like Fraud Watch helps reduce the time it takes to respond to assaults.[297]

3. Pune Citibank MphasiS Call Centre Fraud: Ex-employees of MPhasiS Ltd MsourcE's BPO arm cheated Citibank's US customers to the tune of Rs 1.5crores. It was one of those cybercrime situations that sparked a slew of questions, notably about the role of "Data Protection.The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

   Since any IPC offence committed with the use of "Electronic Documents" might be regarded a crime with the use of "Written Documents," ITA-2000 is adaptable enough to accept parts of crime not covered by ITA-2000 but covered by other statutes. In addition to the part in ITA-2000, terms like "cheating," "conspiracy," "breach of trust," and so on apply in the aforesaid instance.[298]

   The infraction is recognized in both Sections 66 and 43 of the ITA-2000. As a result, the individuals involved are subject to jail, fines, and a duty to pay damages to the victims up to Rs 1crore per victim, for which the "Adjudication Process" can be used.

4. Sony.Sambandh.com Case: In 2013, India received its first cybercrime conviction. It all started when Sony India Private Ltd, which controls the website www.sony-sambandh.com and targets Non-Resident Indians, filed a complaint. NRIs can use the service to transfer Sony products to friends and relatives in India after paying for them online.[299]

   The company guarantees that the products will be delivered to the intended recipients. According to the cybercrime case study, in May 2002, someone using the name Barbara Campa logged onto the website and ordered a Sony

[297] ibid
[298] Cyber Laws and Information Security Advisor, 'Important Cyber Law Case Studies' < https://www.cyberralegalservices.com/detail-casestudies.php > accessed July 21 2021
[299] ibid

Color Television and a cordless headphone. She provided her credit card information and asked for the items to be sent to Arif Azim in Noida. The credit card company cleared the payment, and the transaction was completed. The items were delivered to Arif Azim after the company completed the necessary due diligence and inspection procedures.[300]

The company took digital photographs of Arif Azim accepting the delivery at the time of delivery. The transaction was completed at that point, but after one and a half months, the credit card company alerted the company that the purchase was unlawful because the genuine owner had denied making it.

The company reported internet cheating to the Central Bureau of Investigation, which opened an investigation under Indian Penal Code Sections 418, 419, and 420. Arif Azim was detained once the case was examined. Arif Azim obtained the credit card number of an American national while working at a call center in Noida, which he exploited on the company's website, according to investigations.

In this one-of-a-kind cyber fraud case, the CBI retrieved the color television and cordless headphone.The CBI had enough evidence to prove their case in this case, thus the accused accepted his guilt.

Arif Azim was found guilty under Sections 418, 419, and 420 of the Indian Penal Code, marking the first time that cybercrime has been found guilty.

The court, on the other hand, believed that because the accused was a young boy of 24 years old and a first-time offender, a liberal approach was required. As a result, the court sentenced the accused to a year of probation. The decision has enormous ramifications for the entire country. Apart from being the first cybercrime conviction, it has demonstrated that the Indian Penal Code may be effectively applied to some types of cybercrime that are not covered under the Information Technology Act 2000. Second, a decision like this sends a strong message to everyone that the law cannot be manipulated.[301]

5. SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra: In India's first case of cyber defamation, the Delhi High Court took jurisdiction over a case in which

[300] ibid
[301] ibid

a corporation's reputation was being slandered through emails and issued a significant ex-parte injunction.[302]

In this case, the defendant Jogesh Kwatra, an employee of the plaintiff company, began sending derogatory, defamatory, obscene, vulgar, filthy, and abusive emails to his employers as well as to various subsidiaries of the said company all over the world with the intent of defaming the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a lawsuit seeking a permanent injunction prohibiting the defendant from sending insulting emails to the plaintiff.[303]

It was argued on behalf of the plaintiff that the defendant's emails were clearly obscene, vulgar, abusive, frightening, humiliating, and defamatory. Counsel went on to say that the purpose of sending the emails was to smear the plaintiff's great reputation throughout India and the world. He also claimed that the defendant's actions in sending the emails had amounted to an infringement of the plaintiff's lawful rights.

Furthermore, the defendant has a legal obligation not to transmit the aforementioned communications. It's worth noting that the plaintiff corporation terminated the defendant's employment after discovering the employee may have been sending abusive emails.[304]

The Hon'ble Judge of the Delhi High Court issued an ex-parte ad interim injunction, stating that the plaintiff had shown a prima facie case after hearing the plaintiff's counsel's comprehensive arguments. As a result, the defendant was barred from sending disparaging, defamatory, obscene, vulgar, humiliating, and abusive emails to the plaintiff or its sister corporations around the world, including their Managing Directors and Sales and Marketing departments, in this cyber fraud case in India. Furthermore, the defendant was barred from posting, sending, or causing to be published any information that is disparaging, defamatory, or abusive in the real world or in cyberspace.[305]

[302] ibid
[303] ibid
[304] ibid
[305] ibid

This order by the Delhi High Court is significant because it is the first time an Indian court has taken jurisdiction in a case involving cyber defamation and issued an ex-parte injunction prohibiting the defendant from defaming the plaintiff by sending derogatory, defamatory, abusive, or obscene emails to the plaintiffs or their subsidiaries.[306]

6. Cyber attack on Cosmos Bank: In an extraordinarily daring cyber attack in August 2018, the Pune branch of Cosmos bank was robbed of Rs 94 crores. The thieves were able to move the money to a Hong Kong bank by hacking into the main server. In addition, the hackers gained access to the ATM server in order to obtain information about numerous VISA and Rupay debit cards.

   The switching system, which connects the centralized system to the payment gateway, was hacked, which meant neither the bank nor the account holders were aware of the money transfer.

   According to the transnational cybercrime case study, a total of 14,000 transactions were carried out using 450 cards across 28 countries.

   A total of 2,800 transactions were completed across the country utilizing 400 different cards. This was the first malware attack of its sort, and it effectively shut down all connection between the bank and the payment gateway.

7. BPO fraud: In another MphasiS, India incident, four call center employees obtained PIN codes from four of MphasiS's clients, Citi Group, despite not being permitted to do so. Various accounts were formed in Indian banks under bogus names, and they were able to move money from Citigroup clients' accounts to these accounts using their PINs and other personal information within two months.[307]

   This cyber fraud case occurred in December 2004, but it took the Indian police till April 2005 to locate the perpetrators and make an arrest. It was made feasible thanks to a tip from a US bank when the accused attempted to withdraw money from the phony accounts. Only $230,000 was recovered out

[306] ibid
[307] ibid

of the $426,000 that was stolen. Unauthorized access to carry out transactions was prosecuted against the defendants under Section 43(a).[308]

5.3 CONCLUSION

According to the National Crime Records Bureau, the number of cyber-crimes in India has increased drastically during the last three years. Electronic crime is a major issue. In cases of cyber-crime, banks suffer not only financial losses, but their customers' trust in them is also eroded. It can be concluded that while eliminating and eradicating cybercrime from the cyberspace appears to be an impossible, regular monitoring of financial operations and transactions is doable. The only viable option is to raise public awareness about people's rights and responsibilities, as well as to make law enforcement more hard and strict in order to reduce crime.

[308] ibid

CHAPTER 6

6.1CONCLUSION

Increasing core banking value, revamping the digital agenda, moving from information to insight, dealing with a changing risk regime, transitioning from cash to electronic modes of payment, grappling with financial inclusion, empowering employees, and accelerating innovation are all priorities for banks deploying technology-intensive solutions today. With the rising use of technology, banks have modified their operations and moved towards universal banking. The majority of banks choose cashless and paperless payment methods. Nowadays, banking is referred to as "innovative banking." Banks make use of electronic media to provide a wide range of services.[309]

The banking industry has undergone a paradigm shift as a result of e-banking. Through e- banking, one may readily access their accounts at any time, day or night, using the internet. It facilitates the expansion and development of global trade and business by allowing for the quick transfer of monies anywhere on the planet. It has given the company new dimensions. Because of advancements in information technology and the emergence of e-banking in India, the banking industry has experienced remarkable growth. Banks have benefited from the introduction of e-banking by having lower operating costs, fewer employee requirements, and higher profits. Nonetheless, it comes with a slew of issues, including privacy concerns, security dangers, infrastructure flaws, and so on. E-banking will grow even more if banks carefully consider correct policies and procedures.[310]

Virtual banking has provided banks a boost in providing high-quality service using information technology. With the help of digitalization, we are moving towards a cashless society, which will improve the bank's performance. Nowadays, banks have realized that a banking system without information technology cannot succeed, and this has increased the banking sector's importance in the economy. With the use of electronic banking, all banking transactions may now be completed swiftly and easily. As can be seen from the above data, whether it's ATM deployment, debit and credit

[309] Suhas. D & H. N. Ramesh, "E-banking and Its Growth in India – A Synoptic View" (2018) 5 J Mgmt Res Anal 376
[310] ibid

card issuing, NEFT, RTGS, or Mobile banking (Values and Volumes), we've seen an increase in recent years. Our younger generation has taken banking system changes as a convenience rather than a problem.[311]

E-banking is transforming the banking business, with significant implications for banking relationships and operations. E-banking is the delivery of banking products and services via the internet. Large financial organizations used to have a lot of advantages, but they've lost a lot of them. Customers in the global marketplace now have unfettered access to the internet, which has leveled the playing field. For financial institutions, e-banking is a cost-effective delivery method. Many of the advantages of E-banking are being embraced by consumers. It is a convenient style to have access to one's account via the Internet at any time and from anyplace. As a result, after a bank completes a technology integration plan that allows the customer to access information regarding his or her unique account connection, the bank's internet presence evolves from "broucherware" to "E-banking."

Though there are numerous advantages and opportunities of e-banking but there lies disadvantages too. The most infamous and serious disadvantage of e-banking is cyber fraud. India is seeing a tremendous increase in cybercrime. Cyber criminals frequently commit crimes such as social media, credit card fraud, phishing, and virus, as well as Malware, Denial of service, Gambling, Hacktivist, Personal data leak, corporate data breach, and virtual currency. Males are more likely than females to be involved in cybercrime in the age ranges 18-30. People in their 60s and older are also victims of cybercrime. The fact that senior citizens are also involved in cybercrime is not a good sign. Maharashtra is at the top of the state-by-state list of cybercrime. Nationalized Bank Group is the site of the majority of cybercrime. Money loss and data loss are the most common victims among the many types of banks. Because the internet is a major source of information and a means of communication for people all over the world, it is vital to exercise caution when using it. It is vital to take some precautions when using a computer or the internet to avoid cybercrime. It is critical to educate everyone about cybercrime and penalties, including penalties for safe surfing and browsing, as well as how to use and handle mobile and online banking, how to secure personal information, how to use various applications, and what precautions should be

[311] ibid

taken when conducting online banking transactions. The norms and regulations governing cybercrime must be strictly enforced.

The administration must take real efforts to safeguard the security of the state's digital network and systems, which store critical public information. The lockdown has revealed the government's poor cyber-laws, and following a 5% surge in cyber-crime, the government has moved its attention to this area, with cyber-centers and cyber-police now operational. The government is warning the public not to fall victim to these types of scams and to use caution when entering personal information and passwords on websites. However, the government must enact stricter laws, processes, and techniques to apprehend the hackers. Furthermore, security solutions must be implemented to protect company networks and hospital computers from hackers. These are some of the short-term solutions during the lockdown, however the present Information Technology Act, 2000, needs to be amended because it is a comprehensive act that does not include many of the other areas that are touched by cyber-crime.

Findings

The RBI has produced a number of significant rules for preventing bank fraud that can assist banks in doing so. Internal checks, deposit accounts, administration of check books and passbooks, loans and advances, drafts, internal accounts, and inter branch accounts were all used to assess the level of compliance with these security procedures. The findings of this investigation show that security control procedures are not being followed to their full extent.

6.2RECOMMANDATIONS

The E-Banking market is prohibitively expensive for new entrants, despite the decreased startup costs and fast growth rate. Customer brand preference, existing network, physical presence, security and safety, supplier bargaining power, and non-banking sector rival products have all made the path difficult. However, a newcomer with a unique idea and plan might easily get a foothold in this industry. The analysis of the evolution and current state of E-Banking allows us to make some recommendations to the government, new entrants, and existing e-banks in order to maximize the opportunity to accelerate economic growth.

- Internet penetration is a crucial aspect in E-growth. Banking's according to an OECD study, there is a substantial positive relationship between Internet and E-Banking usage. The trend is usually logarithmic, and for Internet banking to take off, at least 30% of the population must have access to the internet. However, having access to the Internet does not guarantee access to online banking. Companies can provide incentives, such as subsidizing the cost of surfing, free training, numerous access facilities (web, telephone, ATM, etc.), and motivating programs to users and the general populace in this situation, such as in Mexico.
- Customers' account information must be kept private by banks. The RBI has issued a new circular with suggestions for reducing the risk of hacking. However, it is the banker's responsibility to use technology to perform his duties more efficiently. The Reserve Bank of India should also ensure that banks are employing cutting-edge technology. The RBI should appoint technicians and instruct them to file security reports.
- Assigned an auditor to report any theft of funds, no matter how minor. Because electronic banking is undetectable, the risk of bankers misappropriating funds has increased.
- The customer is inconvenienced when the Automatic Teller Machine fails regularly. The number of times banks are not fined for such lapses must be mentioned in the RBI's forthcoming circular. Banks should pay a penalty if they exceed a certain limit, which serves as a reminder to keep an eye on the machine's operation.
- The Consumer Protection Act emphasizes faster and less expensive justice. As previously stated, the Act also applies to banking services. The Act's scope should be extended especially to electronic banking in circumstances of frequent ATM machine failures, security breaches that result in hacking, and exorbitant bank fees for fund transfers, among other things. Despite the fact that this is covered by the RBI circular, it is recommended that they be brought under the purview of the legislation, as this will be more convenient for clients.
- E-banks should make every effort to develop their network as quickly as feasible. Because the majority of clients utilize E-Banking to pay bills, shop,

and so on. As additional third parties join the network, they may be able to attack more customers.

- The majority of "customers" rated ‘privacy and security' as a top priority. It is recommended that banks educate their consumers about this issue in order to raise their awareness. Customers, in particular, are concerned about losing money if their mobile phone is lost (substantial number of respondents worried about it). Second, banks and telecom operators should draft a thorough joint policy on security and privacy so that clients may feel secure when using mobile banking at both the bank and the telecom operator level.

BIBLIOGRAPHY

STATUTES

1. Banker's Book Evidence Act (Act No. 18), 1891
2. Consumer Protection Act (Act No. 35), 1980
3. Income Tax Act (Act No. 43), 1961
4. Indian Penal Code (Act No. 45), 1860
5. Information Technology Act (Act No. 21), 2000
6. Negotiable Instrument Act (Act No. 26), 1881
7. Prevention of Money Laundering Act (Act No. 112), 2002
8. Reserve Bank of India Act (Act No. 26), 1943

BOOKS

1. Dr. J. N. Myneni, "Information Technology Law (Cyber Laws)", Asia Law House, Hyderabad, 2016.
2. Jayaram Kondabagil, "Risk Management in Electronic Banking (Concepts and Best Practices), John Wiley &Sons, Singapore, 2007.
3. Talat Fatime, "Cyber Law in India", Kluwer Law Internatoinal, 2017.
4. Mahmood Shah & Steve Clarke, "E-Banking Management: Issues, Solutions and Strategies", Information Science Reference, US, 2009.
5. R.K.Uppal, "Banking Service and Information Technology", New Century Publications, 2008.
6. Advocate Prasant Mali, "Cyber Law & Cyber Crimes Simplified", Cyber Infomedia), 2017
7. R. K. Uppal, "Modern Banking in India (Dimensions and Risks)", New Century Publications, 2009.

ARTICLES

1. Charan Singh & Deepanshu Pattanayak & Divyesh Satishkumar Dixit & Kiran Antony & Mohit Agarwal & Ravi Kant & S. Mukunda & Siddharth Nayak & Suryaansh makked & Tamanna Singh &Vipul Mathur, "Frauds In The Indian banking Industry", 505, IIMB-WP, 2016, (1-24).
2. Harshita Singh Rao, "Cyber Crime in Banking Sector", Vol. 7, Issue 11, Int'l J Res Granthalayah, 2019, (14-161).
3. A. V. B. N. H. Saroja & Dr.Raavi Radhika, "A Study On Cyber Frauds In Indian Banking Sectors" , Vol.3, Issue 1, IJAASR, 2018, (315-321).
4. Akram Jalal & Jassim Marzooq & Hassan A. Nabi, "Evaluating The Impacts of Online Banking Factors on Motivating the Process of E-Banking", Vol 1, J Mgmt & Sustainability, 2011 (32-42).
5. Rajib Bhattacharyya, "Information technology and Cyber Law : A Globalized Review", Vol. 9, Indian JL & Just, 2018 (115-133).
6. Ms. Neeta & D. V. K. Bakshi, "Cyber Crime in Banking Sector", Vol. 7, Issue 5, AIIRJ, 2009 (25-31).
7. Sikha Kumari & Dr. Ajay Kumar Chattoraj, "E-Banking in India: Present Scenario", Vol.10, Issue 7, UGC Care Group Int'l J & Dogo Rangsang Res J, 2020 (272-284).
8. Jitin Sharma, "A Study of the Present Scenario of E-Banking Service in Indian Market", Vol.2, Issue 1, IJARIIE, 2016 (762-772).
9. Adriana Butcovan, "Banking Security in the Context of International Relation", Vol. 9, Issue 7, Res & Sci Today, 2015 (7-204).
10. Seema Goel, "Cyber Crime: A growing Threat To Indian Banking Sector",Vol. 1, Issue 6, ICRISTME, 2016 (13-20).
11. Soni R.R. & Soni Neena, "An Investigative Study of Banking Cyber Frauds with special reference to Private and Public Sector Banks", Vol. 2, Issue 7, Res J Mgmt Sci, 2013 (22-27).
12. Steve Amchen & Jessica Cordova & Paul Clcero, "Securoies Fraud", Vol. 39, Issue 2, Am Crim L Res, 2002 (1037-1102).
13. Debasree Saha, "Cyber Laws and Banking Frauds with Special Reference to Private and Public Sector Banks", Vol. 3, Issue 9, Int'l J Adv Res, 2016 (10-15).

14. Susan W Brenner & Marc D Goodman, “In Defense of Cyber terrorism: An Argument for Anticipating Cyber Attacks”, Vol. 2, Issue 1, U ILL JL Tech & Pol’y, 2002 (1-59).
15. Subhara Jindal, “Study of E-Banking Scenario in India”, Vol.5, Issue 12, IJSR, 2016 (680-683).
16. Kavunthi Karunakarn, “Role of E-Banking in Current Scenario”, Vol. 6,Issue 2, IJRAR, 2019 (73-76).
17. Joseph & Paul Nolette & & Janine Loaisign Ivanova, “Securities Fraud”, Vol.2, Issue 40, Am Crim L Rev, 2003 (1041-1107).
18. Dr. Manish M. More & Meenakshi P. Jadhav & Dr. K. M. Nalawade, “Online Banking and Cyber Attacks: The Current Scenario”, Vol. 5,Issue 12, IJARCSSE, 2015 (743-749).
19. Miss Prevy Parekh & Miss Tarunya Rao, “Cyber Space & Jurisdiction”,Vol. 2, Issue 5, JCIL, 2019 (1-15).
20. Dr. Adel Azzam Saqf Al Hail, “Jurisdiction in Cyber Crimes: A Comparative Study”, Vo. 22, JL Pol’y G11N, 2014 (75-84).
21. Neha Mehta & Sweety Shah, “Payments Bank: Digital Revolution in Indian Banking System, Vol. 4, Issue 6, IJMH, 2020 (110-114).
22. Surala M S & Dr. Kundan basavaray, “E-Banking Frauds and RBI Guidelines”, Vol. 55, ETIMM, 2019 (409-416).
23. Rohit Jain, “Legal Framework of Internet Banking in India”, Vol. 4, Issue 1, JLL Mgmt Humanities, 2021 (699-711).
24. Dr. Prof. Renu & Kuldeep Singh, “The Impact of E-Banking Service and Customers Satisfaction”, Vol. 3, Issue 4, IJTSRD, 2019 (20-23).
25. Dr. C.P. Gupta & Abhilasha Sharma, “Legal Mechanism of Cyber Crimes Against E-Banking in India”, Vol. 4, Issue 1, IJARCMSS, 2021 (282-286).

NEWSPAPER

1. “Over 290,000 cyber security incidents related to banking reported in 2020”, Business Standard, February 4, 2021.
2. “Rise in cyber crime post Covid is growing risk to bank ratings: S&P”, Business Standard, May 25, 2021.
3. Anto T. Joseph “Why the ATM industry in India continues to struggle” Fortune India, January 7, 2021.
4. “COVID Cyber Crime: 74% of Financial Institutions Experience Significant Spike in Threats Linked To COVID-19 “ Businesswire, April 28 2021

INTERNET SOURCES

1. https://www.cyberralegalservices.com/detail-casestudies.php
2. https://www.legalbites.in/cyber-space-jurisdiction-issues-challenges/
3. https://www.legalserviceindia.com/legal/article-3329-analysis-of-cyber-jurisdiction-in-india.html
4. https://www.mondaq.com/india/financial-services/1048070/rbi-guidelines-for-system-of-security-controls-for-digital-payments
5. https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10477#7
6. https://blog.ipleaders.in/need-know-cyber-laws-india/
7. https://www.mondaq.com/india/finance-and-banking/20687/internet-banking-in-india
8. https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence
9. https://www.appknox.com/blog/cybersecurity-laws-in-india
10. https://blog.ipleaders.in/need-know-cyber-laws-india/
11. https://www.businesswire.com/news/home/20210428005365/en/COVID-Cyber-Crime-74-of-Financial-Institutions-Experience-Significant-Spike-in-Threats-Linked-To-COVID-19
12. http://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html
13. https://www.ijert.org/electronic-banking-in-india-innovations-challenges-and-opportunities
14. https://commercemates.com/features-of-e-banking/
15. https://blog.ipleaders.in/major-legal-issues-indian-e-banking-system/
16. https://www.economicsdiscussion.net/essays/banking-essays/essay-on-internet-banking/17828
17. https://www.fortuneindia.com/macro/why-the-atm-industry-in-india-continues-to-struggle/105011