

**Legal and Regulatory Issues of Cyber Fraud in Transnational  
Banking with special reference to European Union**

A Thesis Submitted

To

**Sikkim University**



In Partial Fulfilment of the Requirement for the  
**Degree of Doctor of Philosophy**

By

**Palchenla Sherpa**

Department of Law

School of Social Sciences

January 2021

6 माइल, सामदुर, तादोंग -737102  
गंगटोक, सिक्किम, भारत  
फोन-03592-251212, 251415, 251656  
टेलीफैक्स -251067  
वेबसाइट - [www.cus.ac.in](http://www.cus.ac.in)



सिक्किम विश्वविद्यालय  
SIKKIM UNIVERSITY

6<sup>th</sup> Mile, Samdur, Tadong -737102  
Gangtok, Sikkim, India  
Ph. 03592-251212, 251415, 251656  
Telefax: 251067  
Website: [www.cus.ac.in](http://www.cus.ac.in)

(भारत के संसद के अधिनियम द्वारा वर्ष 2007 में स्थापित और नैक (एनएएसी) द्वारा वर्ष 2015 में प्रत्यायित केंद्रीय विश्वविद्यालय)  
(A central university established by an Act of Parliament of India in 2007 and accredited by NAAC in 2015)

Date: 11-12-20

CERTIFICATE

This is to certify that thesis titled "Legal and Regulatory Issues of Cyber Fraud in Transnational Banking with Special References to European Union" submitted to the Sikkim University for the partial fulfilment of the degree of Doctor of Philosophy in the Department of Law, embodies the result of bonafide research work carried out by **Palchenla Sherpa** under my guidance and supervision. No part of the dissertation has been submitted for any other Degree, Diploma, Association and Fellowship.

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

We recommend that this thesis be placed before the examiner for evaluation.

Supervisor

Dr. Nidhi Saxena

Assistant Professor

Department of Law

School of Social Sciences

Sikkim University

Head of Department

अध्यक्ष / HOD

विधि विभाग / Department of Law

सिक्किम विश्वविद्यालय

Dr. Prayin Mishra

Associate Professor

Department of Law


School of Social Sciences

Sikkim University

Date: 06/01/2021

### DECLARATION

I, Palchenla Sherpa, hereby declare that the research work embodied in the thesis titled "Legal and Regulatory Issues of Cyber Fraud in Transnational Banking with special reference to European Union" submitted to Sikkim University in partial Fulfilment of the requirement for the Degree of Doctor of Philosophy is my original work. This thesis has not been submitted for any other degree of this University or any other University.



**Palchenla Sherpa**

Ph.D. Registration No.: 17/Ph.D/LAW/03

Registration Date: 22.05.2018

Department of Law

School of Social Sciences

Sikkim University



6 माइल, सामदुर, तादोंग -737102  
गंगटोक, सिक्किम, भारत  
फोन-03592-251212, 251415, 251656  
टेलीफैक्स -251067  
वेबसाइट - [www.cus.ac.in](http://www.cus.ac.in)



सिक्किम विश्वविद्यालय  
SIKKIM UNIVERSITY

6<sup>th</sup> Mile, Samdur, Tadong -737102  
Gangtok, Sikkim, India  
Ph. 03592-251212, 251415, 251656  
Telefax: 251067  
Website: [www.cus.ac.in](http://www.cus.ac.in)

(भारत के संसद के अधिनियम द्वारा वर्ष 2007 में स्थापित और नैक (एनएएनसी) द्वारा वर्ष 2015 में प्रत्यायित केंद्रीय विश्वविद्यालय)  
(A central university established by an Act of Parliament of India in 2007 and accredited by NAAC in 2015)


Date: 05.01.2021

### PLAGIARISM CHECK CERTIFICATE


This is to certify that plagiarism check has been carried out for the following Ph.D thesis with the help of URKUND SOFTWARE and the result is 1 % tolerance rate, which is within the permissible limit (below 10% tolerance rate) as per the norm of Sikkim University.


**“Legal and Regulatory Issues of Cyber Fraud in Transnational Banking with Special References to European Union”**

Submitted by (Palchenla Sherpa) under the supervision of (Dr. Nidhi Saxena, Assistant Professor, Department of Law, School of Social Sciences, Sikkim University) Gangtok, Pin 737101, India.

  
.....  
Signature of the Scholar

Palchenla Sherpa

  
.....  
Countersigned by the Supervisor

  
.....  
पुस्तकालयाध्यक्ष  
Librarian  
Vetted by Librarian 4/1/2021  
केन्द्रीय पुस्तकालय Central Library  
सिक्किम विश्वविद्यालय  
Sikkim University

## CONTENT

Topics	Page No.
<i>Acknowledgements</i>	<i>i-ii</i>
<i>List of Cases</i>	<i>iii-v</i>
<i>List of Abbreviation</i>	<i>vi-viii</i>
<i>Executive Summary</i>	<i>ix-xi</i>
<b>CHAPTER ONE</b>	<b>1 - 29</b>
1.1. Introduction	1 - 9
1.2. Operational Definition	10 - 12
a. Computer	
b. Computer System	
c. Computer-related Fraud	
d. Computer Emergency Response Team (CERT)	
e. Computer Forensic	
f. Cyber Security	
g. Electronic Evidence	
h. Electronic Channel	
i. Electronic Record	
j. Internet	
k. World Wide Web	
1.3. Statement of Problem	13 - 19
1.4. Review of Literature	19 - 27
1.5. Rational & Scope of Study	27 - 28
1.6. Hypothesis	28
1.7. Research Objectives	28
1.8. Research Questions	29
1.9. Research Methodology	29
<b>CHAPTER TWO: LEGAL AND REGULATORY STRUCTURE</b>	<b>30- 77</b>
2.1. Introduction	30- 34
2.2. Legal and Regulatory Structure of Indian Banking	34
2.2.1. Reserve Bank of India Act, 1934	35 - 39
2.2.2. Banking Regulation Act, 1949	39 - 42
2.2.3. Indian Contract Act, 1872	42 - 46
2.2.4. Indian Penal Code, 1860	46 - 48
2.2.5. Indian Evidence Act, 1872	49 - 53
2.2.6. Information Technology Act, 2000	53 - 60

2.2.7. National Cyber Security Policy, 2013	60 - 62
2.3. Legal and Regulatory Structure of European Banking Industries	62 - 65
2.3.1. European Banking Authority	65 - 66
2.3.2. European Central Bank	66
2.3.3. Single Rule Book	67
2.3.4. Council of Europe's Convention on Cybercrime	67 - 74
2.4. Comparison of Indian Banking System with European Union	74 - 77
<b>CHAPTER THREE: ISSUES OF CYBER FRAUDS</b>	<b>78 - 138</b>
3.1. Introduction	78 - 81
3.2. Fraud and Cyber Fraud: Definitional Issues	81 - 84
3.2.1. Essentials of Cyber Fraud	84
3.2.2. Types of Cyber Fraud	85 - 102
3.3. Investigation Mechanism and Issues	102 - 106
3.3.1. Electronic or Digital Evidence	106 - 108
3.3.2. Collection of Electronic Evidences	108 - 109
3.3.3. Extraction of Electronic Evidence	109 - 110
3.3.4. Maintaining Privacy of Individual	110 - 111
3.3.5. Search and Seizure of Electronic Evidence	111 - 113
3.3.6. Challenges during Electronic Investigation	113 - 116
3.4. Prosecuting Issues	116 - 118
3.5. Issues of Consumer Liability	118 - 122
3.6. Transnational Issues	122 - 123
3.6.1. Legal Provisions to Collect Information from Outside India	123 - 125
3.7. Jurisdictional Issues	125 - 135
3.7.1. Mutual Legal Assistance	135 - 137
3.7.2. Uniform Cyber Fraud Law	137 - 138
<b>CHAPTER FOUR: ROLE OF RBI</b>	<b>139 - 158</b>
4.1. Introduction	139 - 142
4.2. RBI in Traditional Banking	142 - 144
4.3. RBI IN Electronic Banking	135 - 158
<b>CHAPTER FIVE: JUDICIAL TRENDS IN EUROPEAN UNION</b>	<b>159 - 182</b>
<b>CHAPTER SIX: CONCLUSION &amp; SUGGESTION</b>	<b>183 - 199</b>
<b>REFERENCES</b>	<b>200 - 226</b>

## **ACKNOWLEDGEMENTS**

Firstly, I would like to express my gratitude to my supervisor Dr. Nidhi Saxena, Assistant Professor, Department of Law, Sikkim University, Gangtok, for her continuous intense guidance, support, constructive comment, and motivation during my Ph. D Course. Her sincere monitoring and encouragement made work complete with perfection. Since she has been a significant source of inspiration in my academic journey, I couldn't imagine having a better mentor for my Ph. D Course. She has been my source of motivation throughout the research work. Thank you, mam, for believing me and my process of working. I will remain obliged towards her and always consider your suggestions throughout my life.

Besides the supervisor, I would like to convey my sincere gratitude to all the faculty members, the Department of Law, Sikkim University, Dr. Pravin Mishra, Prof. Imtiaz Gulam Ahmed, Dr. Veer Mayank, Dr. Denkila Bhutia, Dr. Sonam Yangchen for their support and guidance. I express my sincere gratitude towards advisory members to provide me with valuable suggestions and inspirations during research. I am grateful to all my Sikkim University teachers because you all are the ones who introduced me to the new world of research and academics.

I would also like to express my gratitude to Mr. T.T. Sherpa, Headmaster from my primary school, from whom I got to know about the higher Ph. D. studied when I was in class VII. Sir, it was because of your thought I got my dream of pursuing a Ph.D. I would also like to thank Mr. Mingma Sherpa (my papa my inspiration), Mr. L.O Sherpa, and Mrs. Bimla Rai (My teachers from Khop Primary School). Because of

your blessing and guidance, a girl from a remote village can achieve her dream. Thank you very much once again.

Further, I would like to thank entire non-teaching faculty members of the Law Department and the library staff of Sikkim University for providing support and guidance while researching for the research materials.

My acknowledgment couldn't be complete without thanking my dear friends, Punam Thapa, Shradjanjali Rai for supporting me during my Ph.D. Shargam Subba, thank you for your care and support throughout my journey and accompanying me in midnight writing.

Thanks to Dr. Deepanker Rai, my senior cum, good friend, who has been there to boost and support me with his advice. Special thanks to Dr. Ajit Mishra for your bits of advice and encouraging me in completing my thesis.

Last but not the least, I am grateful to my parents, Momma, Papa, and Uru, for showing me unconditional support, encouragement, and sacrifices during the entire journey. I am thankful to my brother Dr. Palzor Sherpa and my Lil sister Mingkila Sherpa for taking care of our family on my behalf. Thank you, my beautiful aielas Seema Lepcha, Chomit Lepcha, Chokit Lepcha, and Pema Dichen Sherpa. Also, Mingma Yangri Sherpa (sano aunty) and Lakpa Sherpa (uncle), thank you very much for supporting me in times of thick and thin. With the blessing of almighty and from all my family members, friends, I had accomplished my work.

- **Palchenla Sherpa**



## LIST OF CASES

1. Aayush Kumar v. State of Bihar 2020 SCC Online Pat 684
2. Abhinav Gupta v. JCB India Ltd. decided on 1 September 2010
3. Abdul Rahaman Kunji vs The State Of West Bengal on 14 November
4. Abolade Bpde v. First Bank of Nigeria Plc. & MasterCard West Africa Limited  
Unreported Suit No: FHC/L/CS?405/13, delivered on 10 April 2019
5. Ali Ibrahim vs. the State of Kerala on 14 October 2014
6. Anvar P.V v. P.K.Basheer, on 18 September 2014 (2014) 10 SCC 437
7. Bhagwandas Goverdhandas Kedia v. M/S. Girdharilal Parshottamdas 1966 AIR  
543, 1966SCR (1) 656
8. CBI vs. Arif Azim, 2003
9. Chandrabai Bhoir v. Krisnna Bhoir AIR 2009 S.C. 1645 Bom
10. Chief Engineer Hydel project v. Ravinder Nath AIR 2008 SC 1315
11. Citi Group Inc. and Others v. Citi Finance Service and Another
12. Digital Equipment Corp. v. Altavista Technology, Inc. 960 F. Supp. 456 (Decided  
on March 12, 1997)
13. DVA Public School v. The Senior Manager, India Bank, Midnapur Branch & Ors.  
CIVIL APPEAL NO. 9352 of 2019
14. Entores Ltd. v. Miles Far East Corpn., (1955) 2 QB 327
15. Gafar v. Government of Kwara State (2007). 4 N.W.L.R (Pt. 1024) 37
16. Guaranty Trust Bank v. Motunrayo-Tolulope Aloegen (nee Oyesola), unreported  
SUIT No: CA/L/461/2016 delivered on 1 March 2019
17. Hirday Nath Roy v. Ramchandra Barna Sarma AIR 1921 Cal 34 (FB)

18. Himanshu Sarkar v. State Bank of India & Another. District Consumer Disputes Redressal Commission (19 August, 2014)
19. ICICI Bank Ltd v. Official Liquidator of APS Star Industries Ltd (2010) 10 SCC
20. ICICI- Pune Bank Fraud case
21. Jagdeo Singh v. the State and Ors. (MANU?DE/0376/2015)
22. Jawala Bank Ltd. vs. Shitla Parshad Singh AIR 1950 AII 808
23. Justice K. S. Puttaswamy v. Union of India (2017) 10 SCC 1
24. Kharak Singh v. Union of India 1963 AIR 1295, 1964 SCR (1) 332
25. MacDonough v. Fallon MacElligott Inc. 1996 U.S. Dist. Lexis 15139 (S.D.Cal. August 5, 1996)
26. Manager Axis Bank Ltd., v Sai Sandeep Bhosle AIR 2017
27. Mobarik Ali v. The State of Bombay AIR 1957 S.C. 857
28. NASSCOM v. Ajay Sood and Ors 119 (2005) DLT 596, 2005 (30) PTC 437 Del
29. Ostern Pvt. Ltd. & Anr v. State of West Bengal & Ors AIR 2014
30. Pune Citibank MphasiS Call Center Fraud
31. Puneet Mittal v. State Bank of India Order dated 31st January, 2015
32. Rubi (Chandra) Dutta v. United India Insurance Co.Ltd. (2011) 11 SCC 269
33. R v. Cochrane, 1993, United Kingdom
34. S.P.C. Naidu v. Jaganath, AIR 1994 S.C.853
35. State of Andhra Pradesh v. T. SuryachandraRao, AIR 2005 S.C. 3110
36. Senior Branch Manager, United Bank of India v. Binoy Kumar Roy, Order dated 03.01.2017
37. Societe Des Products Nestle S.A and Anr vs. Essar Industries and Ors 2006 (33) PTC 469 Del
38. SIL Import v. Exim Aides Silk Exporters, 1999 (2) KLT 275 (SC)

39. Sukhlal v. Tara Chand, (1950) ILR 33 Cal 68 (FB)
40. Swaran Sabharwal vs. Commissioner of Police, 1998 Criminal Law Journal 240  
1990 68 Comp Cas 652 Delhi
41. Subba Rao v. State of Andhra Pradesh (2013) 2 SCC 162
42. State of Andhra Pradesh v. T. Suryachandra Rao, AIR 2005 S.C. 3110
43. State v. Mohd. Afzal and Ors (2003) DLT 385, 2003 (71) DRJ 17
44. State of Punjab & Ors v M/S. Amritsar Beverages Ltd. & Ors decided on 8  
August, 2006
45. State Bank of India v. Chander Kalani & Ors. Cyber Appeal No. 13 of 2015 (m.  
A. No.282 of 2017)
46. State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru (2005) 11 SCC 600
47. State Bank of India (Code No. 05604) Through Its Branch Manager, RRL Jorhat  
Branch, District-Jorhat-785006 Assam v. Dr. J.C.S Katakya NH-37, At Road, Near  
Neist Gate No. 1, Jorhat Assam 2017 SCC Online NCDRC 1093
48. Tony Enterprise v. Reserve Bank of India on 11 October 2019
49. Umashankar Sivasubramanian v. ICICI Bank, Petition No. 2462 of 2008
50. Union of India v. Chandha (WN) 1933 Cri LJ 859 (SC)
51. Xxx v. State Bank of India & 2 Ors, AIR 2013
52. Zippo Mfg. CO. v. Zippo Dot Com Inc., 952 F. Supp. 1119 (W. D. Pa. 1997)

## ABBREVIATION

AIR	: All India Report
ATM	: Automated Teller Machine
ACPO	: Association of Chief Police Officer
B.C	: Before Christ
BSNL	: Bharat Sanchar Nigam
CBI	: Central Bureau of Investigation
CCTV	: Closed-circuit Television
CD	: Compact Disc
CEO	: Chief Executive Officer
CERT-IN	: Indian Computer Emergency Response Team
CSC	: Card Security Code
Cr. P. C	: Criminal Procedure Code
CNP	: Card Not Present
CPC	: Civil Procedure Code
CTS	: Cheque Truncation System
CVC	: Central Vigilance Commission
CVV	: Card Verification Value
DCBs	: District Cooperative Banks
DSP	: Deputy Superintendent of Police
DSCI	: Data Security Council of India
EBA	: European Banking Authority
ECS	: Electronic Clearing Service
ECB	: European Central Bank
EBT	: Electronic Banking Transaction
EFT	: Electronic Fund Transfer

E-Banking	: Electronic Banking
EU	: European Union
EWS	: Early Warning Signal
E-wallet	: Electronic wallet
FIR	: First Information Report
GOI	: Government of India
HTML	: Hypertext Markup Language
IPC	: Indian Penal Code
IT Act	: Information Technology Act
ICT	: Information Communication Technology
ICCPR	: International Convention on Civil Right
ICICI	: Industrial Credit and Investment Corporation of India
IMF	: International Monetary Fund
INR	: Indian rupee
IP	: Internet Protocol
IS	: Information Security
IVR	: Interactive Voice Response
KYC	: Know Your Customer
MHA	: Ministry of Home Affairs
MLA	: Mutual Legal Assistance
MLAT	: Mutual Legal Assistance Treaty
MPIN	: Mobile Personal Identification Number
MSIE	: Microsoft Internet Explorer
NCIIPC	: National Critical Information Infrastructure
NEFT	: National Electronic Fund Transfer
NASSCOM	: National Association of Software and Service Companies
OTP	: One Time Password

PIL	: Public Interest Litigation
PKI	: Public Key Infrastructure
PIN	: Personal Identification Number
PPI	: Prepaid Payment Instrument
RBI	: Reserve Bank of India
RFA	: Red Flagged Account
RTGS	: Real Time Gross Settlement
SBI	: State Bank of India
SC	: Supreme Court
SCC	: Supreme Court Cases
SIM	: Subscriber Identity Module or Subscriber Identification Module
SMS	: Short Message Service
SOC	: Security Operations Centre
SRM	: Single Resolution Mechanism
SSM	: Single Supervisory Mechanism
SSL	: Secure Socket Layer
StCBs	: State Cooperative Banks
SWIFT	: Society for Worldwide Interbank Financial Telecommunications
WWW	: World Wide Web
TCP	: Transmission Control Protocol
TDSAT	: Telecom Dispute Settlement and Appellant Tribunal
UCBs	: Urban Cooperative Bank
UDHR	: Universal Declaration on Human Right
UIDAI	: Unique Identification Authority of India
UPI	: Unified Payment Interface
URL	: Uniform Resource Locator
USB	: Universal Serial Bus

## EXECUTIVE SUMMARY

This thesis work is divided into six chapters dealing with various aspects that are covered in the research work. The research work is based on the following hypothesis:

1. The significant growth in cyber frauds is a threat to security for the electronic banking transactions.
2. The existing legal framework is inadequate to deal with cyber frauds in banking.

The first chapter “Introduction,” enunciates the problem of the study in the area of legal and regulatory issues of cyber fraud, research objectives and research questions. The chapter contains the detailed methodology applied during the progress research. The chapter also provides an overview of literature of the study.

The second chapter is “Legal and Regulatory Structure”. This chapter covers the legal and regulatory issues of banking law and specifically discusses the legal measures of India and European Union. This chapter addresses the first research objectives of the research i.e., to know what various elements should be included in the definition of ‘Cyber ‘Fraud’. The definition of ‘cyber fraud’ has not yet been incorporated till date in any existing laws. The chapter also deals with the deficiencies in existing legislation and their inadequacy in regulating the growing issues and concerns of cyber frauds in banking. The research after examining various legal instruments finds that the Budapest Convention of European Countries is the sole instrument at the international level which deals with cybercrime in an international scenario. The European countries have common laws designed in conformity with the Budapest Convention and thus avoided the issues of conflicts of laws amongst European nations. The chapter analyses various provisions of cyber crime convention and associated aspects.

The third chapter is “*Issues of Cyber fraud*” This chapter covers the various issues of cyber fraud including the definition of cyber fraud, the issues relating to investigation and prosecution of cyber fraud, the liability of banks towards its customers when they avail various internet banking services duly offered by the banks. The chapter also covers the transnational issues of investigation and prosecution including conflicts of laws. This chapter explores the second research objective i.e., the existing investigating mechanism in the cases of cyber fraud and the difficulties faced by investigating and prosecuting authorities. The chapter analysis issues and provides the probable solutions for them. The finding of the chapter can be expressed as “the various issues of cyber frauds originate from the definition itself which is missing in the Indian laws. Thus accomplishing the first step of giving definition may lead to the resolution of many associated issues. Further, it is found that the liability of banks towards its customers is not fixed which results in no remedy to the customers. Thus fixing the liability of banks reduces the number of cases of cyber fraud.

The fourth chapter is “*The Role of RBI*” which covers the role of RBI (Reserve Bank of India) in the banking industry, especially in internet banking. The chapter observes that the advanced economy has made a shift from traditional banking to internet banking using digital innovations. Reserve bank monitors and reviews the legal requirement for internet banking. It laid down various policies, guidelines, procedures which need to be followed for the detection, investigation, prevention, and reporting of various types of bank frauds in particular online frauds. RBI as a regulator has made substantial improvements in time of advancement in technology by establishing efficient and secure functioning which has further helped in development in the internet banking system in India. Further, the chapter also covers the security mechanism which is provided by RBI in cases of cyber fraud in banks and the



procedures in case of failure of non-applicability of the rules and notification issued by RBI.

The fifth chapter is “*Judicial Trends in India and European Union*”. This chapter covers various judicial pronouncements of the court in India as well as by the courts of different countries. The chapter also examines to what extent the laws so enacted has upgraded and updated to handle the cases of cyber fraud in the banking industry. The chapter covers the effect and the development of laws. Even though India has adequate criminal statutes and procedures along with well trained investigating agencies it is still not possible to combat cyber crime committed beyond the geographical boundaries of the country. The jurisdiction issues are mainly caused by a lack of criminal statutes on online banking frauds as well as improper implication of Information Technology Act, 2008, lack of procedural laws in particular standard procedure for the search & seizure and analysis of digital evidence. There is always a need for mutual assistance regarding investigation with regards to the collection of data stored in computers and the interpretation of content data. India needs to be a part of global villages having a common criminal policy to combat cybercrime that is where Budapest Convention has its role to play.

The sixth chapter is “*Conclusion and Suggestion*” this chapter concludes the thesis and provides suggestions after analysis of each and every aspect, the various data collected during the writing of my thesis. An attempt has been made to point out the inadequacy of present legislation for the cyber fraud issues and provides few suggestions to combat raising issues of cyber fraud. Thus research concludes as both the hypotheses in the research work have been proved.

**“Legal and Regulatory Issues of Cyber Fraud in Transnational  
Banking with Special Reference to European Union”**

**CHAPTER ONE**

**1.1. Introduction**

Technology adoption has brought the world closer; it has changed the way of living. It has the possibilities to exchange information more often. Banking system has shifted from traditional banking to electronic banking. The banking industries are exploiting technology in order to provide best services and for reaching their customers. Technology has brought electronic banking services making the banking environment more customer friendly as well as proficient. Technology advancements in the banking sector have created better customer friendly services making it convenient to transfer money or purchasing goods and services at any time. Banking services provided via the internet or online banking is easiest and the cheapest channel for delivering banking services. “When we look into the banking history it has shown past records of lending, exchanging and accepting of money, which prove that the banking system was well set in the old days. Banking history can be traced back to 2000 BC in temples of Babylonian and commercial banking along with investment was started from twelfth century Italy.”<sup>1</sup> “The old famous temples in ancient Greece are Ephesus, Delphi and Olympia and the king used temples as a banker to their people.”<sup>2</sup> The term “bank” is used throughout the world. “Bank” as a term has

---

<sup>1</sup>Roussakis, E. N. (1997), Global banking: origins and evolution. URL:<http://www.scielo.br/pdf/rae/v37n4/a06v37n4.pdf>

<sup>2</sup>S. S Kaptan, (2003) Indian banking in electronic era. Sarup & Sons

originated from different terms such as Banque, Banca or a Bench. It accepts public deposits as well as exchanges the amount and lends them back in time of requirement.

Banking in India has its own history. The money-lending activities are considered as having associations with the Vedic period. During the time of Ramayana and Mahabharata era, the bank itself started to work full-fledged. The bankers in the Manusmriti period performed most of the functions of the modern banks, such as accepting of deposits, providing loans, granting the loans to the king in times of great crisis, issuing and managing the currency of the country.<sup>3</sup>

Modern banking in India started at the beginning of the 19th century. The earliest bank of India was established by the East India Company. Whereas, the Bank of Hindustan was the first joint stock bank set up in 1770. After the Bank of Hindustan, “the Bank of Bengal, Bank of Bombay and Bank of Madras were set up which were known as Presidency banks.”<sup>4</sup> They continued till 1921, and came to be known as Imperial Bank of India after they were merged together. In 1934 the Reserve Bank of India was set up as per the order issued by the Royal Commission on Indian Currency and Finance.<sup>5</sup> In 1949, the Banking Regulation Act was passed for the purpose of regulation and supervision of banks.<sup>6</sup> Bank Nationalization was another milestone in the development of the banking system in India. The Imperial Bank was later changed into the State Bank of India in 1955 and along with it eight banks were nationalized in 1960 and later in the 1980s seven more banks were nationalized. Due to

---

<sup>3</sup>*Supra* 2

<sup>4</sup> <https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20-Professional.pdf>

<sup>5</sup> Banking Systems in India (Hilton- Young Commission) URL: <http://www.yourarticlelibrary.com/banking/reserve-bank/reserve-bank-of-india-originand-development/26356>

<sup>6</sup>*Supra* note 5

nationalization, the whole structure of the banking system changed and it helped to further expand their branches in other areas.<sup>7</sup>

Before introducing electronic banking, traditional banking required a physical present in the bank for simple tasks like getting bank statements. Electronic banking has made it possible where we can conduct our banking task with the internet connection mobile having a particular payment transaction application. Both the bank and customers are taking advantage of online services without any hassle. Technology has provided everything just within our comfort space and it has proved to be a boon for our society moving ahead towards digitization society. Advancement in technology has changed everything including people's routine life. The most drastic impact of technology advancement is on the banking system and their service delivery channels. It has completely transformed the banking pattern of conducting their banking business. Banks are utilizing these opportunities to create more new convenient and customer friendly services. Adoption of the concept of electronic/ internet banking shifts the whole banking scenario, it's time saving and cost reduction allowing banking anytime anywhere.

In the 1980s online banking was started where online banking simply meant the usages of computer keyboards and terminals which were needed in order to access the account. Adoption of internet banking has allowed changing the definition of banking by inclusion of electronic payment systems providing customers to avail financial transactions through the internet.<sup>8</sup> Adoption in new updated technology has transformed the banking system and brought competition within their business, facing

---

<sup>7</sup> Karishma Bhandari & Harvinder Soni, "Indian Banking Sector: Then, Now & the Road Ahead", International Research Journal of Engineering and Technology (IRJET), Vol.3 Issue.4, April.2016

<sup>8</sup>History of Online banking: How Internet Banking Went Mainstream by Ruth Sarreal, October 7, 2017 URL: <https://www.gobankingrates.com/banking/history-online-banking/>

new digital challenges. Technology brought swiftness in banking business and their modes of communicating methods to their customers via different new service delivery channels. This reduces transaction cost, saves time in completing banking business and most of the financial institutions/ organizations perform their business through internet banking. Every individual as well as society at large has been dependent on internet banking. This brought the world closer, by bringing it under the same umbrella of the banking system.<sup>9</sup> Everyone got dependence on technology so no one can think about doing banking business without technology; even they cannot isolate themselves from using technology. The dependence on technology has created numerous challenges before regulators because of its advancement leading towards cyber fraud.

The shift of banking technology has witnessed the transformation in their services providing new modes of facilities through technology. The threat of cyber fraud has emerged as a new digital crime with the advancement of technology. This has created security issues for customers relating to their accounts in the bank. Information available online is vulnerable which can be misused by the predators for making unauthorized internet transactions. There is no legal framework for cyber fraud in India in absence of that it has been creating challenges to the regulator and government.<sup>10</sup>

The rapid adoption of advanced technology in banking has created a threat to the privacy of individuals. Sensitive information like user name, bank account number, passwords are stored in computers while using internet banking, those sensitive

---

<sup>9</sup>E- Banking URL: <http://shodhganga.inflibnet.ac.in/bitstream/10603/89802/4/chapter%202.pdf>

<sup>10</sup> R. R Soni and Neena Soni, *An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks*, Vol. 2(7), 22-27, July (2013), Research Journal of Management Sciences

information's are at risk. It can be hacked by hackers at any time through the internet which may lead to acts of cyber fraud which is rising at an alarming rate and creating serious concern.

India has passed regulation governing computer fraud in 2000 in the form of Information Technology Act, 2000. But they have failed to include cyber fraud in the ambit of Information Technology Act 2000. There is no such Act which can provide a specific definition for cyber fraud. It has been problematic to understand the elements constituting cyber frauds. The Information Technology amendment Act of 2008 also remains inadequate to deal with issues of cyber fraud. They had failed to provide specific definitions or particular sections dealing with cyber fraud. Even Penal laws along with other legislation fail to provide any definition for cyber fraud.

Indian existing laws are dealing cyber fraud cases with the provided provisions to similar offences such as cheating, fraud, and misrepresentation etc., provided by Indian Penal Code 1860, Indian Contract Act of 1872. In absence of definition it hampers the whole procedure of investigation and makes it delay for announcement of verdict. It's been important to define cyber fraud and to clarify the elements constituting cyber fraud in order to know the parameters for the cyber fraud elements. Fraud is an unfair deception in order to make gain unlawfully from another party. In fraud, a fraudster with dishonest intention tries to convince the victim over communication through which they can gain a profit amount from the loss of the victim.<sup>11</sup>

---

<sup>11</sup>Palchenla Sherpa, Cyber Fraud in Banks: New Dimensional Crime, Muktsabd Journal URL:203july2020.pdf (shabdbooks.com)

To understand cyber fraud we must know the different elements of cyber frauds and methods which make it different from traditional fraud. Fraud involves criminal intention for deception so that they can gain financial profit. Internet technology as a tool has proven to be the easiest method for committing fraud. According to the Oxford dictionary fraud must contain willful deception with criminal intention resulting into personal gain financially.<sup>12</sup> These activities will only benefit the fraudster. With the development of internet and internet users fraudsters are learning new *modus operandi* so that they can easily fool the public for getting access to have unauthorized transactions. The Indian Contract Act, 1872 has defined the term “Fraud” “Which means to deceive intentionally the other party or their agent according to their connivance.”<sup>13</sup>

Fraud covers more meaning as provided by the definition in the act. Elements which are essential for fraud are the presence of false statements and having wrongful intentions. Reserve Bank is the Central Bank for the Indian banks and it is considered to be the regulator of the bank which provides different guidelines, notification for the functioning of the bank smoothly. Being the regulator of all banks, the Reserve Bank has not defined fraud in any of their guidelines or policies regulated for the working of banks. The RBI in context of electronic banking suggested that any person that

---

<sup>12</sup>Oxford dictionary defines “fraud” as a wrongful or criminal deception intended to result in a financial or personal gain. See: Oxford Dictionary of English published by Oxford University Press 2010

<sup>13</sup>“Section 17 of Indian Contract Act, 1872: “Fraud” defined- “Fraud” means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract

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

Explanation- Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak, or unless his silence, is, in itself, equivalent to speech.

commits fraud within the banking transaction through a computer system where it results in monetary loss to the bank.<sup>14</sup>

‘Fraud’ has not been directly defined under Indian Penal Code 1860, it has provided some relevant sections for punishment to those acts which lead to the commission of fraud. Other sections that are similar to fraud are dealing with Fraudulently,<sup>15</sup> Cheating,<sup>16</sup> forgery,<sup>17</sup> concealment,<sup>18</sup> counterfeiting,<sup>19</sup> misappropriation of property<sup>20</sup>

---

<sup>14</sup>Frauds in the Banking Sector: Causes, Concerns and Cures (Inaugural address by Dr. K. C. Chakrabarty, Deputy Governor, Reserve Bank of India on July 26, 2013 during the National Conference on Financial Fraud organized by ASSOCHAM at New Delhi) Dated: Jul 29, 2013 URL: Reserve Bank of India - Speeches (rbi.org.in)

Working group on Information Security, Electronic Banking, Technology Risk Management and Cyber Fraud has suggested a definition on fraud wherein they included the element of a deliberate act of omission that may result to wrongful gain to some person/s which may for a temporary period or otherwise.

<sup>15</sup>“Fraudulently” under section 25 of the Indian Penal Code defines which states as “A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise”.

<sup>16</sup>section 415 stated that “Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any person, or to consent that any person shall retain any property, or intentionally induce the person so deceived to do or omit to do anything which he would not do or harm to that person in body, mind, reputation or property, is said to “cheat”.

Explanation- A dishonest concealment of facts is a deception within the meaning of this section.

<sup>17</sup>Section 463 of Indian Penal Code, 1860: Forgery- [Whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

<sup>18</sup>Section 120 of Indian Penal Code, 1860: Concealing design to commit offence punishable with imprisonment- Whoever, intending to facilitate or knowing it to be likely that he will thereby facilitate the commission of an offence punishable with imprisonment, voluntarily conceals, by any act or illegal omission, the existence of a design to commit such offence, or makes any representation which he knows to be false respecting such design, if offence be committed; if offence be not committed- shall, if the offence be committed, be punished with imprisonment of the description provided for the offence, for a term which may extend to one-fourth, and, if the offence be not committed, to one-eighth, of the longest term of such imprisonment, or with such fine as is provided for the offence, or with both.

<sup>19</sup>Section 28 of Indian Penal Code, 1860: Counterfeit- A person is said to “counterfeit” who causes one thing to resemble another thing, intending by means of that resemblance to practise deception, or knowing it to be likely that deception will thereby be practised.

[Explanation 1- It is not essential to counterfeiting that the imitation should be exact.

Explanation 2- When a person causes one thing to resemble another thing, and the resemblance is such that a person might be deceived thereby, it shall be presumed, until the contrary is proved, that the person so causing the one thing to resemble the other thing intended by means of that resemblance to practise deception or knew it to be likely that deception would thereby be practised.]

<sup>20</sup>Section 403: Dishonest misappropriation of property- Whoever dishonestly misappropriates or converts to his own use any movable property, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Illustrations:



and breach of trust.<sup>21</sup> The provisions dealing for crime related internet fraud provided in section 43(d), 65 and 66 of Information Technology Act, 2000.

“However, the Indian existing enacted law or legislation is inadequate in order to deal with cyber fraud. They might have not thought that cyber fraud would create challenges before lawmakers while framing the Information Technology Act, 2000. Information Technology Act, 2000 is the single act in India that covers all the crime related to computer and information technology. It is only punishable for the theft, cheating, fraud etc., under Indian Penal Code, 1860. Every day cyber fraud rates are increasing and the only Information Technology Act, 2000 is insufficient in order to deal with cyber fraud. Therefore, in order to face the challenges of new digital crime, cyber fraud the new law has to be framed for efficient handling. David Bainbridge points out that cyber fraud contains dishonest intentions of a person for stealing money by using a computer as a tool and directs the system for making fraudulent transactions sometime through cloned ATM or debit/credit card.<sup>22</sup>

“The banks and other largest financial institutions are the first large-scale computer users for making salary payment and other accounting functions. Therefore, fraud in a

---

(a) A takes property belonging to Z out of Z's possession, in good faith believing at the time when he takes it, that the property belongs to himself. A is not guilty of theft; but if A, after discovering his mistake, dishonestly appropriates the property to his own use, he is guilty of an offence under this section.

(b) A, being on friendly terms with Z, goes into Z's library in Z's absence, and takes away a book without Z's express consent. Here, if A was under the impression that he had Z's implied consent to take the book for the purpose of reading it, A has not committed theft. But, if A afterwards sells the book for his own benefit, he is guilty of an offence under this section.

<sup>21</sup>Section 405 of Indian Penal Code, 1860: Criminal breach of trust- Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits “criminal breach of trust”.

<sup>22</sup> Supra note 11 See: URL: <http://shabdbooks.com/gallery/203-july2020.pdf>

computer scheme emerged.”<sup>23</sup> The nature of technological devices is borderless and in such a situation this threat becomes a serious issue. With regard to the existence of international instruments

The Council of Europe’s Convention on cybercrime (Budapest Convention) is the first recognized international treaty for cybercrimes. Cyber fraud as a crime evolved only after people started adopting technology for their convenience and if we look into the present scenario, every individual is dependent mostly on technology for everything. The fraudsters are taking advantage of those things and gaining money out of many account holders. The jurisdiction has always been an issue while dealing with cyber fraud. Cyber fraud involves many jurisdictions creating difficulties for handling the cases. Even in international level jurisdiction issues are unsolved. There is no uniform cyber law which can solve these issues. There is a lack of harmonized law at the international level. Every nation has their own domestic law that governs computer crime but when it comes to international level there is a conflict of law for governing the accused of cyber fraud. It proves that the enacted regulation is insufficient as well as inadequate for new digital crime of cyber fraud. “The new digital modes of fraud are hindering the establishment and industries in their development. The amount of money being lost fraudulently is still on the rise even though various safety measures are provided by the RBI to all the banks. Cyber fraud is easy to conduct. These crimes are challenging the stability and integrity of a country.”<sup>24</sup>

---

<sup>23</sup>Cyber Space Jurisprudance, Vardhaman Mahaveer Open University, Kota URL: PGDCL01.pdf (vmou.ac.in)

<sup>24</sup> (Inaugural address by Dr. K.C. Chakrabarty, Deputy Governor, Reserve Bank of India on July 26, 2013 during the National Conference on Financial Fraud organized by ASSOCHAM at New Delhi) *Supra* note 12

## **1.2. Operation Definition**

Following relevant terms are used in the study:

### **a. Computer:**

“Computer means any electronic, magnetic, optical or other high speed data processing device or system which performs logical arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.”<sup>25</sup>

### **b. Computer System:**

“A device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.”<sup>26</sup>

### **c. Computer-related fraud:**

The causing of loss of property to another by manipulating or altering, deleting any computer data, with fraudulent or dishonest intention to gain economic benefit without right, is considered as computer-related fraud.

---

<sup>25</sup> Section 2(1)(i) of Information Technology Act, 2000

<sup>26</sup> Section 2(1)(l) of Information Technology Act, 2000

**d. Computer Emergency Response Team (CERT):**

Computer Emergency Response Team (CERT) is an organization that studies computer and network in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security

**e. Computer Forensic:**

Computer Forensic is a computer application for computer investigation and analysis techniques in order to obtain potential legal evidence. It is a new branch connecting law with digital or electronic evidence as it could be presented before the court of law.<sup>27</sup>

**f. Cyber Security:**

“Cyber Security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.”<sup>28</sup>

**g. Electronic Evidences:**

“Electronic Evidence is data which is manipulated, stored or communicated via any man-made device such as computer or computer system or transmitted over communication systems, which are admissible in court of law.”<sup>29</sup>

---

<sup>27</sup>Computer forensics is a discipline which combines elements of laws and computer science in order to collect and analyse collected data from computer systems, networks, wireless communications, and storage devices in a way it can be admissible as evidence before the court of law. Computer Forensics US-CERT URL: <https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf>

<sup>28</sup>Section 2(1)(nb) of Information Technology Act, 2000

**h. Electronic Channel:**

Electronic channel is the method by which banking services are provided to the customers using electronic devices. It is the technical channel of delivering services which offer better benefit of service distribution. Electronic channels have been considered to be more efficient in terms of delivery.

**i. Electronic Record:**

“Electronic records mean data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.”<sup>30</sup>

**j. Internet:**

“The Internet is the largest computer network in the world, connecting millions of computers. The Internet has the ability to interact and share information whenever it's required. It allows people to connect and communicate with everyone.”<sup>31</sup>

**k. World Wide Web:**

“World Wide WEB or WWW is an organized reservoir of information. It is a collection of documents that are linked together in an almost endless manner. It is

---

<sup>29</sup>Dr. Swarupa Dholam, “Electronic evidence and its challenges”, URL: [http://mja.gov.in/Site/Upload/GR/Title%20NO.129\(As%20Per%20Workshop%20List%20title%20no129%20pdf\).pdf](http://mja.gov.in/Site/Upload/GR/Title%20NO.129(As%20Per%20Workshop%20List%20title%20no129%20pdf).pdf)

<sup>30</sup>Section 2(1)(t) of Information Technology Act, 2000

<sup>31</sup> The Internet, URL: <https://ncert.nic.in/textbook/pdf/kect107.pdf>

composed of thousands of computers on the internet which contain varying degrees of information which can be assessed by internet account holders.”<sup>32</sup>

### 1.3. Statement of Problem

Over 25, 800 online banking fraud cases were reported in 2017 in India. As per the data provided by RBI in December 2017, the fraud related to ATM or credit or debit cards and by net banking were total 10,220 in number. This reporting of RBI is alarming and may lead to loss in customer faith over information technologies and newly introduced advanced banking services. There are certain identified nomenclature used to refer to some banking related criminal activities like Cyber squatting, Phishing, however these terminologies are not used or identified under Information Technology Act, 2000 of India. Cyber squatting, Phishing, are a kind of fraud committed with the help of computer technology with the profit motives or intention of monetary gains. Here cyber squatting refers to illegal domain name registration while, Phishing is a twofold crime which is being used in order to obtain sensitive banking account information such as usernames, passwords, credit card details etc.<sup>33</sup> and then to use the same for the further commission of the crime. Here the *modus operandi* includes that the wrongdoer often directs the users to enter or release personal information by deceptive means or techniques and then use of these obtained information for their benefits or satisfying the desired objective. Therefore the first challenge in the issues of electronic banking fraud is to understand what actually constitutes cyber fraud and also to find out what parameter does it constitute cyber fraud. Indian Laws have remained silent for cyber fraud. Since the existing laws in India have no definition of Cyber fraud i.e. there is no any available legal definition

---

<sup>32</sup> K Mani, Electronic Banking Frauds [ATM, Mobile, Banking and Internet Banking] published by Kamala Publishers, Edition 2016.

<sup>33</sup> [http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018\\_.pdf](http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018_.pdf)

of cyber frauds. The Indian Contract Act, 1872 defines fraud under Section 17 but its definition is limited where it covers fraud in case of agreement or contract only.<sup>34</sup> Another definition which can be referred is given under Indian penal code. There is a shift of performing criminal acts with the medium of advanced computer technology. Essential elements for cyber fraud must have electronic transactions as a mode or medium in fraudulent banking transactions. In ‘Budapest Convention on Cybercrime’, 23.XI.2001, the definition of cyber fraud is not provided so it lacks even international directives on the issue. In Article 8<sup>35</sup> of the convention had discussed computer related fraud but is not about banking fraud. It is worth to mention that United States Computer Fraud and Abuse Act of 1986<sup>36</sup> provided additional penalties for fraud and related activities related to computers but it also does not provide a specific definition of cyber fraud. Section 1030 of Computer Fraud and Abuse Act deals with Fraud and related activity in connection with computers.

In the absence of any definition under existing law categorizing any act as cyber fraud is difficult. There is also difficulty in illustrating the definition of cyber frauds since finding and including the elements of cyber frauds is a challenge. The main issue is to ascertain whether cyber fraud is a crime that is mediated through technology or is it exclusively technology crime? Cyber fraud is a crime as it contains both the *mens rea* and *actus reus* to prove their criminal liabilities. There is no specific definition of cyber fraud and defining cyber fraud has become a key analytical problem.

---

<sup>34</sup>Supra note at 10

<sup>35</sup>Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data;  
b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

<sup>36</sup>The Computer Fraud and Abuse Act (CFAA) is a United States cyber security bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984.

In the absence of definition investigation is another challenge. Computer crimes are different from usual crimes so the investigation also needs to be done differently. There are no eyewitnesses, no documentary evidence or no usual evidentiary clues. Investigation of cyber fraud will be in progress only when police departments are well equipped and competent. The qualification of investigating authority is given under IT Act and he should not be below the rank of Sub Inspector for the criminal cases. The main objective of investigation of any crime/cyber fraud is to collect evidence and use the same in prosecution of the offender and get the remedy to the victim of cyber fraud. The reasons for the failure of investigation in case of cyber fraud are:

- a). Challenge to understand whether any particular act (cyber fraud) amounts to crime under any existing category of crime;
- b) The investigating officers are not well trained and in the absence of proper ideas regarding technology they failed to identify evidence. They don't understand what constitute an evidence, challenges are even in collection and preservation due lack of an understanding of computer forensics;
- d). The cyber evidence has always remained fragile in nature which can be tempered and destroyed easily by predators and they being expert in using computer technology are always using new modes of modus operandi which makes them one step ahead of investigating authorities.
- e). The other crucial issues in this line is the short supply of manpower to handle cyber related crime/ cyber fraud and they are unable to recruit the best available IT experts in the department. This leads to the danger of appointing untrained and



incapable personnel in carrying the investigation of cyber fraud. The security control guidelines provided by Reserve Bank of India are not been compliance properly.

Cyber frauds are hi-tech faceless crimes which do not limit itself within the boundaries, which makes it difficult to investigate. Absence of a proper guidance manual for cyber fraud investigation makes it more complicated for further investigation.

The next issues/ problem are Reporting Mechanisms for Cyber fraud which still lack the customer awareness on the issues for the reporting where they left uninformed or unreported to the investigation authority. Due to fear of negative exposure victims are not coming forward to register a crime. Sometimes in lack of awareness people don't even realize that they are the victims of cyber fraud. Investigating and supervisory bodies like Central Vigilance Commission (CVC) or Central Bureau of Investigation (CBI) are already over burdened with many pending investigations and have limited resources at their disposal. Most of the bank frauds are detected very late and those fraudsters get enough time to wipe their trail and that makes it very difficult to prove their criminal intent because of non availability of evidence and witnesses.

Cyber fraud dealing agencies are not well aware about the proceeding, they are not sufficient in themselves to deal with the faceless crime of cyber fraud. There is an absence of a specified department dealing with cyber fraud matters. Central Bureau of Intelligence and Police who presently handle the cyber fraud are not able to focus completely because they have to investigate all the people of multiple departments of the bank where they lack in coordination resulting in further delay in investigation. People are still unaware regarding cyber fraud which is the reason for them being victims of cyber fraud. Victims of cyber fraud are unwilling to come forward to file

complaints because of embarrassment they are feeling to inform others about them being the victim. There are procedural lapses in identifying the various causes which are responsible for bank frauds. The best way to prevent frauds is by identifying why it is happening?

Guidelines for security control have been issued by the Reserve Bank of India that needs to be followed by all banks but unfortunately they fail to provide the penalties towards the banks on the failure of non compliance. RBI lack to mention the bank regarding the consequences they will be bearing on the failure to comply with the applicability of the guidelines properly. Therefore due to his serious gap security control guidelines have not been compliance properly in the banks. Also the bank employees work under pressure and they are not able to scrutinize the documents properly on their own. The bank employees in the absence of any proper guidelines and directions lack awareness on these issues; even they are properly trained for handling these issues.

“Bank authorities are unable to recruit trained experienced staff. They are posting inexperienced new staff in high positions where they are not able to deliver their services and they are inadequate to handle the new dimensional crime such as cyber fraud. Technology related fraud is primarily due to unsteadiness of banks in complying guidelines or policies framed by RBI or failure to maintain the standard procedures and system in the bank by their employees. Banks are unable to install early warning signals of frauds in order to detect early fraud.”<sup>37</sup>

The banks had not employed the best available technology system and data analytics in order to ensure effective implementation of the red flagged account and early

---

<sup>37</sup>*Supra* note 10

warning signals framework as suggested by Reserve bank of India. The bank has not equipped them with the experts to be deployed to track activities of borrowers and to make an early detection of fraud. Many times the staff themselves does not know the exact definition of fraud. Employees are not being kept updating and providing them with the classes with regards to banking frauds. The Bank management has failed to implement guidelines or policies within their staff where in case of deficiency while delivering banking transactions services act negligently or fraudulently. The people are still unaware about the authenticated methods of using internet banking safely. The authentication methodology involves One Time Password (OTP), which is used to authenticate the account and the OTP so generated remains for 60 seconds. Biometrics technology is used to authenticate the identity of a living person with the help of fingerprints, iris configuration, and facial structure. Although the biometrics technology for security has not been properly set up because it is expensive and every customer cannot afford these security systems. Though there were known cases of fraud in the sector, one major question still remain unanswered, which is: what is the nature, immediate and remote causes of fraud, and how can it be prevented?

It is not an easy task to deal with cyber fraud as it is committed by more than one or two persons together with varying responsibilities in commission. Cyber fraud being borderless crime is very difficult and complicated to investigate. It involves multiple countries' jurisdiction and multiple numbers of parties that created confusion to differentiate the place of origin of the act of cyber fraud for jurisdiction purposes. In spite of having provisions on extraterritorial crime but in reality there is no applicability of law. Numerous jurisdictions of the countries had created uncertainty about the applicability of enacted laws. National boundaries have thus created serious obstacles and there is absence of harmonious law for cross-border coordination for

conducting investigation or sharing information for court proceedings. Uniform cyber laws are required to combat the unavoidable crime of cyber fraud which needs to be brought under control before it creates huge damage to the individual or banking financial institution and economic growth.” Therefore calls for research on the issues.

#### **1.4. Review of Literature**

The World literatures are ample, though not saturated, that focused on the issues of cyber fraud in banking industries and specifically legal and regulatory issues in India are missing, though the entire analysis has not been done as a whole in any single piece of work. A few researchers exclusively investigated on the various issues of cyber fraud in the banking industries in India and other countries. After reading a number of research papers, reports, RBI orders, and surveys etc., the review of literature has been thematically organized in a way and manner which this research aims to fulfill. Literature review has been woven around the three main sub-themes- firstly, the emergence of banking system, reasons and the issue emerging in the absence of definition of cyber fraud and possible elements for defining the same; secondly the issues of investigation and prosecution of cyber fraud and thirdly, in the absence of any legal and regulatory measure against cyber fraud the cross borders issues in banking industries.

1. L.S. Hoskote (1996),<sup>38</sup> in his article “*Crime and Security in Electronic Banking*”, has discussed in length how the evolution from barter system to gold, then to paper money and then to plastic money has taken us today to electronic cash, banking and fund transfer and automated teller machines.

---

<sup>38</sup> L.S. Hoskote, “*Crime and Security in Electronic Banking*”, January 1996, CBI Bulletin Vol. IV

However with the introduction of electronic money the issues of technology clothed crime also evolved.

2. Karishma Bhandari & Harvinder Soni,<sup>39</sup> “*Indian Banking Sector: Then, Now & the Road Ahead*”, the author has basically discussed the banking system in ancient India and how it started with money lenders accepting deposits and issuing receipts in their place. With nationalization of banks it marked an exemplar shift of banking standard from class banking to mass banking. The major changes in the banking sector are due to financial inclusion and technology. Technology has been proved to be a crucial element for improving productivity and rendering efficient customer service.
3. Dr. Roshan Lal & Dr. Rajni Saluja,<sup>40</sup> “*E-Banking: The Indian Scenario*”, the author pointed out that banking services are now accessible 24x7 and even banking services are done just with a single touch. We found less currency than debit/credit cards in our wallet. So, this huge part of changes is due to the initiation of information technology. IT has upgraded our banking system and their services but along with these it has also been facing a threat from cyber fraud.
4. Ashu Khannaand & Bindu Arora (2009),<sup>41</sup> “*A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry*”, they have focused on the reason how banks frauds are committed but they have missed how they should take the raising alert of

---

<sup>39</sup>Bhandari Karishma & Harvinder Soni, “*Indian Banking Sector: Then, Now & the Road Ahead*”, International Research Journal of Engineering and Technology (IRJET), Vol.3 Issue.4, April.2016

<sup>40</sup> Dr. Roshan Lal & Dr. Rajni Saluja, “*E-Banking: The Indian Scenario*”, Asia Pacific Journal of Marketing & Management Review, Vol.1 (4), December (2012)

<sup>41</sup>Ashu Khanna & Bindu Arora, “*A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry*” Int. Journal of Business Science and Applied Management, Volume 4, Issue 3, 2009.

banks frauds seriously and need to ensure that there is no looseness or lack of strictness in internal control mechanism. It is clearly seen that there is a lack of awareness level of bank employees regarding frauds and they do not have favorable attitudes towards RBI procedure. There are still lacks of training, competition and low compliance levels which are framed by the Reserve Bank of India. However the paper does not provide any legal modification if and how.

5. Zarka Zahoor, MoinUd-din and Karuna<sup>42</sup>(2016), "*Challenges in Privacy and Security in Banking Sector and Related Countermeasures*", with the extensive use of technology particularly the internet, banking is becoming more dependent on technology. Unfortunately, with this cyber-crimes related to banks are increasing stupendously. Banking industry has been exposed to a large number of cyber-attacks on their data privacy and security such as frauds with online payments, net banking transactions, electronic cards etc. The paper also says the main reason behind these institutions is to gain confidential data or steal money from banks, but what is the modus operandi is not discussed which could help in overcoming the challenges.
6. Aaron M. French (2012),<sup>43</sup> "*A Case Study on E-Banking Security- When Security Becomes Too Sophisticated for the User to Access Their Information*", the paper brings a new factor that organizations, online banking in particular, are spending the majority of their efforts on external security without properly assessing the importance of internal security. With internal

---

<sup>42</sup>Zarka Zahoor, MoinUd-din and Karuna, "*Challenges in Privacy and Security in Banking Sector and Related Countermeasures*", International Journal of Computer Applications, Volume No 144 – No.3, June 2016

<sup>43</sup> Aaron M. French, "*A Case Study on E-Banking Security- When Security Becomes Too Sophisticated for the User to Access Their Information*", Journal of Internet Banking and Commerce, August 2012, vol. 17, no.2

security being of a higher risk than external security, these additional security measures give users a false sense of security. The study tries to address the need for increased awareness of internal threats through security measures such as security awareness, policies, practices, and procedures. Online banks and other organizations should evaluate every aspect of security bearing in mind the user security as the final objective. According to the researcher, while security is important, organizations should balance the need for increased security with the desire to make systems easy to use and useful to the consumer and not prohibit them from accessing their information.

7. Dr. A. Prasanna,<sup>44</sup> “*Cyber Crime: Law and Practice*”, she has basically discussed the various kinds of cyber frauds and many cases related to it. In her article we can clearly see that there is insufficient law for cyber frauds, which cannot be only covered under the Information Technology Act 2000. So we can see that Indian Penal Code can apply to certain categories of cybercrime. Even after having many legislation and Acts we can say that there is still need to upgrade that legislation to take control over the alarming growth of crime.
8. Seema Goel,<sup>45</sup> “*Cyber-Crime: A Growing Threat to Indian Banking Sector*”, Law enforcement should reconsider new digital crime which targets banks and huge financial institutions. The motive of cyber criminals will always be the financial gain. It creates many legal issues for the regulator too so before it gets late Law enforcement agencies need to develop new measures in order to combat cyber fraud.

---

<sup>44</sup> <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>

<sup>45</sup> Seema Goel, “*Cyber-Crime: A Growing Threat to Indian Banking Sector*”, International Journal of Science Technology and management Vol.No.5, Issue No.12, December 2016 available at <http://data.conferenceworld.in/IFUNA18DEC16/P13-20.pdf>

9. Shewangu Dzomira,<sup>46</sup> in his article “*Electronic Fraud (Cyber Fraud) Risk In The Banking Industry, Zimbabwe*”, discussed the forms of electronic fraud that has been carried out in banks and challenges faced by them. Even though technology has made it more convenient to the people, sometimes in an attempt to maximize the benefit of technology most of the people end up being a victim of technology. The challenges faced by the banks are technical disadvantages, lack of knowledge and awareness, and lack of legal legislation. Although paper pointed out various categories of electronic frauds but an emphasis on the elements of frauds is not included.
10. Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas,<sup>47</sup> in “*The Effects of Cyber Threats on Customer’s Behaviour in e-Banking Services*,” emphasizes cybercrime is one of the burning issues in the online banking industry in the world. All financial institutions must be aware of online threats and they must have taken all the security measures to improve and maintain their financial stability. To understand the security concern one needs to understand the methods and tactics adopted by cyber fraudsters, which they can use for fraudulent activities. The paper opens the door for further investigation of tactics applied by the fraudsters in different cases.
11. Soni R.R. and Soni Neena,<sup>48</sup> in “*An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks*”, says the relevant security mechanism is not properly followed by private banks

---

<sup>46</sup>Shewangu Dzomira, “Electronic Fraud (Cyber Fraud) Risk In The Banking Industry, Zimbabwe”, Risk governance & control: financial markets & institutions / Volume 4, Issue 2, 2014

<sup>47</sup>Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas, “The Effects of Cyber Threats on Customer’s Behaviour in e-Banking Services”, International Journal of e-Education, e-Business, e-Management and e-Learning Volume 7, Number 1, March 2017

<sup>48</sup> R.R. Soni and Neena Soni, “An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks”, Research Journal of Management Sciences, Vol. 2(7), 22-27, July 2013



whereas the public sector banks still follow the old traditional approach. The paper gives a comparative study of bank frauds between public and private banks, and concludes frauds are mostly done in private banks as compared to public banks.

12. Sanchi Agrawal,<sup>49</sup> in “*Cyber Crime in Banking Sector*”, points out that banks have expanded their services and provided better facilities through technology but cyber crime has always remained an issue. She also says that even setting up a cyber cell which monitors crime is not leading to an increase of the reporting of crime owing to the reason that either they are staying in a remote area or due to unawareness regarding the report to be placed. She also points out the inadequacy in provision of IT Act with extra- territorial jurisdictional issues. But research does not suggest what should be added in the existing provisions of IT Act.

13. Ompal, Tarun Pandey, Bashir Alam,<sup>50</sup> “*How to Report Cyber Crimes in Indian Territory*”, discusses various services offered by the banks after technological advancement in the banking sector and the paper also emphasizes the shift from physical threats to cyber crime threats in banking matters. The paper discusses the role of many bodies dealing with cybercrime all over the world like in India CERT-IN (Indian computer emergency response team)

---

<sup>49</sup>Sanchi Agrawal, “*Cyber Crime in Banking Sector*”, Volume 3, May (2016)

<sup>50</sup>Ompal, Tarun Pandey, Bashir Alam, “*How to Report Cyber Crimes in Indian Territory*”, International Journal of Science Technology and Management, Vol. No. 6, April 2017

14. Ahmad Kabir Usman and Mahmood Hussain Shah,<sup>51</sup> “*Critical Success Factors for Preventing e-Banking Fraud*”, says in his article that bank stakeholders are constantly implementing a new security system to eradicate e-banking frauds. Consequently, there is still need for research to narrow down the specific area for further improvement. The paper emphasizes that the banks need to be active and create or modify their policies, procedures and technologies according to new development and emerging concerns.
15. Reserve Bank of India with references to the guideline of Cyber Security Framework in Banks<sup>52</sup> has stated that banks should immediately place the cyber-security policy in an appropriate approach to combat cyber threats. It has also given the emphasis for the Cyber Security Policy that needs to be distinct and separated from the broader IT policy/ IS Security policy so that it can highlight the risks from cyber threats and the measures to address these risks. However the guideline doesn't contain the provision of non compliance.
16. Dr. M. Imran Siddique, Sana Rehman,<sup>53</sup> “*Impact of Electronic Crime in Indian Banking Sector – An Overview*”, the important aspect in Indian banking sector is to make banking transactions free from electronic frauds. Banking sector is coming with numerous changes and electronic fraud presents a high level of risk. Nowadays, electronic crimes are increasing very fast with the help of information technology and at the same time the evolution of law is very slow.

---

<sup>51</sup> Ahmad Kabir Usman and Mahmood Hussain Shah, “*Critical Success Factors for Preventing e-Banking Fraud*”, Journal of Internet Banking and Commerce, Vol. 18 No.2, August 2013

<sup>52</sup>RBI Guideline Vide Circular DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016

<sup>53</sup>Dr. M. Imran Siddique, Sana Rehman, “*Impact of Electronic crime in Indian Banking Sector- An Overview*”, International Journal of Business Information Technology, Vol. 1 No.2 September 2011

17. Suneet Dwivedi,<sup>54</sup> “*Jurisdictional Issues in Cyber Crime*”, the problem with jurisdiction of cyber crime is that it is still a debatable one which remains unsolved till date. Lack of uniform cyber law is creating difficulties for investigation.
18. Yougal Joshi, Anand Singh,<sup>55</sup> “*A Study on Cyber Crime and Security Scenario in India*”, the research paper points out that the IT Act came with legalization of electronic records and amended several existing laws. However the amendment in the IT Act in 2008 was to make it more compatible with the laws globally.
19. Cameron S. D. Brown,<sup>56</sup> in “*Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*”, says that without universal cyber crime conventions, the conflict of law will always create dilemma for the applicability of law without damaging other parties or individuals. Cyber crime cases demands for cooperative mechanisms that are not provided in the existing law create difficulties for the police. Many cyber crime offenders have evaded the prosecution due to the weakness in the law as that does not provide technological means of offences. However how to amend the existing laws was not yet discussed.
20. B.R. Sharma,<sup>57</sup> “*Bank Frauds including Computer and Credit Cards Crimes Prevention and Detection*”, 2<sup>nd</sup> Edition, Universal Law Publishing, computer

---

<sup>54</sup>Suneet Dwivedi, “Jurisdictional Issues in Cyber Crime”, available at [https://www.academia.edu/3700793/Jurisdictional\\_Issues\\_in\\_Cyber\\_Crime](https://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime)

<sup>55</sup>Yougal Joshi, Anand Singh, “*A Study on Cyber Crime and Security Scenario in India*”, International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013

<sup>56</sup> Cameron S. D. Brown, “Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice” International Journal of Cyber Criminology Vol. 9 Issue 1 January – June 2015

<sup>57</sup>B. R. Sharma, “*Bank Frauds including Computer and Credit Cards Crimes Prevention and Detection*”, 2<sup>nd</sup> Edition, Universal Law Publishing

crimes are different from usual crime and no eyewitnesses are found, no usual evidentiary clues, no documentary evidence as these crime has conducted in cyberspace which is not visible for us to witness. Cyber crime is difficult to investigate.

21. Sukanya Kundu & Nagaraja Rao,<sup>58</sup> “*Reasons of Banking Fraud- A Case Of Indian Public Sector Banks*”, bank fraud is difficult to detect and with the passage of time it is difficult to trace the culprit. The banker does not have enough time to scrutinize documents thoroughly. The bank's frauds are caused because of ignorance, situational pressures and permissive attitudes.

22. P.S. Lokhande, Dr. B.B. Meshram,<sup>59</sup> “*Collecting Digital Evidence: Internet Banking Fraud - Case study*”, the author stated that online banking fraud is becoming very common and it is easily done through modern technology. So there is no formal technical knowledge as to deal with online fraud cases. There is a huge problem to establish evidence since there are no such eyewitnesses. Even the sufficient and proper forensic knowledge is not there with the employee and they are not been able to set proper investigation plans

### **1.5. Rational and Scope of Study:**

Most of the time, scholars have only focused on cybercrime-related issues, but they forget to focus solely on cyber fraud. Cyber fraud is one of the most cybercrimes committed in the present day. They failed to address the issue and problems of cyber fraud, which is growing with technology development as a new dimensional crime in

---

<sup>58</sup>Sukanya Kundu & Nagaraja Rao, “*Reasons Of Banking Fraud – A Case Of Indian Public Sector Banks*”, International Journal of Information Systems Management Research & Development (IJISMRD) Vol. 4, Issue 1, Jun 2014

<sup>59</sup> P.S. Lokhande, Dr. B.B. Meshram, “*Collecting Digital Evidence: Internet Banking Fraud - Case study*”, International Research Journal of Engineering and Technology (IRJET)Volume 2 Issue 2 May 2015

India. This study may help policymakers to formulate comprehensive policies to address the cyber fraud problem faced in the virtual world, which is an urgent need even in India. During the course of study it focuses on the following research questions along with objectives.

**1.6. Hypothesis:**

1. The significant growth in cyber frauds is a threat to security for the electronic banking transactions.
2. The existing legal framework is inadequate to deal with cyber frauds in banking.

**1.7. Research Objective:**

1. To know what various elements should be included in the definition of Cyber Fraud which is not yet been incorporated in any existing laws.
2. To know the existing investigating mechanism in the cases of cyber fraud and to find out the difficulties faced by the investigating and prosecuting authorities with the objective of proposing the probable solutions.
3. To identify the various banking procedural lapses in electronic banking transactions.
4. To study the deficiencies in existing legislations and their inadequacy in regulating the growing issues and concerns of cyber frauds in banking.
5. To find out the adequacy of international instruments concerning the cyber related crimes in electronic banking specifically in the transnational matters and to suggest the legal improvements with extra territorial perspective.

### **1.8. Research Questions:**

1. In the absence of specific legal definition of cyber fraud, what various elements would constitute the definition of cyber fraud?
2. What is the investigative mechanism in the absence of legal definition of cyber frauds to ensure justice? What various techniques for collection of electronic evidence in the cases of cyber frauds investigation are adopted by investigative authority?
3. The banks are upgrading their security system under the supervision of RBI yet what are the causes for various procedural lapses in conducting e-banking and to what extent RBI guidelines can provide security to the bank customer against Cyber fraud?
4. Whether the existing international law is adequate to deal with cyber related crimes in e-banking considering the issues of extra territorial jurisdiction?

### **1.9. Research Methodology:**

The researcher has adopted a doctrinal method for completing entire research work. For that primary source, I had referred to different Acts, Legislations, Regulations, various notifications, and Orders issued by RBI during the course of time, Case studies, Conventions and laws, and judgments of different countries which relate to cyber frauds. For secondary sources like books, articles, journals, etc that had been referred for conducting the study. Further, she has referred to different judgments passed by Indian courts as well as foreign courts for the cases of bank fraud through the medium of internet such as phishing, cheating, credit/debit card frauds/ vishing etc.

## CHAPTER TWO

### LEGAL AND REGULATORY STRUCTURE

#### 2.1. Introduction:

Today, “banks have become synonymous with technology and have leveraged Information Technology (IT) in all areas of governance, operations, and control.”<sup>60</sup> Information technology is playing an important role by providing better banking services to its customers. Banking is the backbone of an Indian economy; it is playing a vital role for the economy's growth and development. Indian banking has undergone tremendous changes with the up-gradation of information technology. With the adoption of technology upgradation in the banking system, it has become easier to conduct banking transactions with simple touch. Technological adoption in the banking system removed the monotonous, time-consuming tasks, reduced human error, and extended access to banking related facilities. Technology has shifted banking in paperless banking done without physical existence in banks. Also provides customer information that it would be much more expensive to deliver on a person-to-person basis. The new easiest and convenient service of internet banking attracts the customers for availing the services. Numerous facilities are provided by banks with adoption of advanced technology which made it possible to reach out to their customers even in rural areas.

“India moving towards the digitalization era, contributed to the rapid growth of banking business but cyber fraud started taking place all over the world affecting the

---

<sup>60</sup>*Supra* note 4

growth of the economy. Individuals must have internet connection web browser software in order to access their account and make other banking transactions.

Internet banking is emerging as convenient system doing banking online with help of available electronic channels without much difficulty. Automated Teller Machine (ATMs) is the most used service by the customer to access money anytime or anywhere without making any trip to the banks. It is the most popular and convenient delivery channel. The Electronic Clearing Service (ECS) and National Electronic Fund Transfer (NEFT) are new electronic modes of payment transaction services provided by banks.<sup>61</sup> “Electronic Clearing Services is a new mode of electronic payment or receipt where anyone can make transactions from their one bank account to another.”<sup>62</sup> “Electronic Clearing Services are used by large institutions for transferring bulk payments in their department or organization.”<sup>63</sup> “National Electronic Funds Transfer (NEFT) is a payment system through which individuals, firms, or corporate can transfer the funds from any bank branch.”<sup>64</sup>

Bank has also provided other payment transaction services via, Electronic Bill Payment, Electronic Fund Transfer (EFT), Account Opening Request, Account Statement and Transaction Enquiry. Every bank has developed their own genuine banking mobile application which can be downloaded from Google play store. Through these mobile applications we can even apply for loans online which get sanctioned without any hassle. They have provided every facility such as providing mini statements of banks can check all the past transaction details, insurance facilities

---

<sup>61</sup> Dr. Roshan Lal & Dr. Rajni Saluja, “E-Banking: The Indian Scenario”, Asian Pacific Journal of Marketing & Management Review, Vol. 1(4), December 2012 URL: <http://indianresearchjournals.com/pdf/APJMMR/2012/December/2.pdf>

<sup>62</sup>[https://www.business-standard.com/article/pf/what-is-electronic-clearing-service-ecs-111070800019\\_1.html](https://www.business-standard.com/article/pf/what-is-electronic-clearing-service-ecs-111070800019_1.html) 20th January, 2013

<sup>63</sup>What is Electronic Clearing Service (ECS)? | Business Standard News (business-standard.com)

<sup>64</sup>*Supra* note 4 at 54



are also provided. Banking is now very customer friendly which is not limited within paper and banking hours, it's now 24 X 7 service. Customers are taking full advantages of new services provided by internet banking.

There are both advantages and disadvantages to the introduction of technology in the banking system. The necessitate forcing the statute to enact laws for appropriately regulating internet banking in the banking system. Law cannot be expected to be rigid with the change of technology. Its recent failure of the legislation for internet governing laws has shown its inadequacy and vulnerability. The complexity of security and privacy issues of individuals are mostly arising in electronic banking activity.<sup>65</sup> Adoption of LPG has brought changes in the banking system. Traditional banks slowly started transforming into digital banking with the adoption of advanced technology. Cyber fraud affects not only the banks; it also affects the people, society, and our economy.

Until the early '90s the traditional banking model was prevailing, but after that, internet banking services were started. The Indian government enacted the Information Technology Act, 2000, and thereafter in order to look at different aspects of electronic banking, RBI created a committee for electronic banking.”<sup>66</sup> According to Essinger (1999), Internet banking is: "to give customers access to their bank accounts via a web site and enable them to enact certain transactions on their account, given compliance with stringent security checks.<sup>67</sup> In electronic banking, it does not involve any kind of physical exchange of money, and it's done electronically with the help of using the internet. It provides a universal connection from any location

---

<sup>65</sup> *Supra* note 10

<sup>66</sup> <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0>

<sup>67</sup> Kamau, Denis Mburu, “*Effects Of Technological Innovations On Financial Performance Of Commercial Banks In Kenya*” October 2013

worldwide and is universally accessible from any internet-linked computer. Therefore, internet banking can be denoted as delivery of banking services through internet. The scope of internet banking is still evolving.

Cyber fraud often makes headlines news daily as a new digital crime that is growing in our society.<sup>68</sup> It is a white-collar crime growing with the internet. Digital transactions are adopted by every financial institution which puts it at risk for cyber fraud and has increased the crime. The victims do not disclose most cyber frauds “because of the fear of losing confidence, trust, image, and business in society. The major area of fraud is conducted by misusing credit cards by obtaining passwords by hacking, misrepresentation, and transfer of funds, deceptive investment newsletters containing false information about companies, etc.”<sup>69</sup>

Internet banking is an extension of traditional banking, where they use the internet as a medium for delivering their services to customers. The laws that are applicable to the traditional banking activities are also equally relevant to internet banking. The law includes Reserve Bank of India Act, Indian Contract Act, 1872, 1934, Banking Regulation Act, 1949, Indian Evidence Act, 1860, Information and Technology Act, 2000, and Indian Penal Code, 1860. Information and Technology Act, 2000 deals with all kinds of offences related to computers in India. But cyber fraud as an offence has not been defined in the act. In its absence, it has been difficult for law enforcement agencies to deal with accused convicted under the different cyber fraud offences because they have not framed the IT Act by including cyber fraud within their ambit.<sup>70</sup> The Reserve Bank of India (RBI) and Government of India (GOI) policy has

---

<sup>68</sup> The Indian Express dated: March 32, 2020

<sup>69</sup> <http://shabdbooks.com/gallery/203-july2020.pdf>

<sup>70</sup> Dr. Verma Amit and Simi K. Bajaj, “*Cyber Fraud: A Digital Crime*” 2008 [https://www.academia.edu/8353884/CYBER\\_FRAUD\\_A\\_DIGITAL\\_CRIME](https://www.academia.edu/8353884/CYBER_FRAUD_A_DIGITAL_CRIME)

considerably helped”<sup>71</sup> in the “growth of internet banking in India. There are many reforms taken by the Reserve Bank of India for the inclusion of internet banking in the banking system. There has been a rise in the question of the adequacy of law to deal with technology- driven situations such as denial of services or data corruption because of technology failure or hacking.”<sup>72</sup>

These chapter discuss the Legal and regulatory structure of banking industries in India and the European Union. The first part will discuss in detail the provisions of banking laws regulatory measures in India. Similarly, the second part will discuss the provisions of banking laws regulatory measures in European countries. The third part will be a comparative study of India and European countries' banking sectors.

## **2.2. Legal and Regulatory Structure of Indian Banking Industries.**

The existing enacted laws in India are inadequate while dealing with cyber fraud. Adoption of electronic banking brought new challenges, before the law enforcing agencies. The safety of customer interest and their account with the bank from fraudulent activities remains a big concern.<sup>73</sup> Earlier, Cyber fraud was not in the picture on whose basis the laws can be framed for dealing cyber fraud in India. Therefore, it is needed to regulate new law including cyber fraud law to provide justice to victims and control its growth.

---

<sup>71</sup> *ibid*

<sup>72</sup> *Supra* note 70

<sup>73</sup> Edwin Agwu & Mercy Agumadu, "Analysis of the Emergent Issues in Internet Banking Adoption in Nigeris", *European Journal of Social Science*, Vol. 52 No 2, June 2016 available at <http://www.europeanjournalofsocialsciences.com>

### 2.2.1. Reserve Bank of India Act, 1934.

The Reserve Bank of India (RBI) as India's central bank and as a regulator<sup>74</sup> of banks & bankers etc. controls the country's financial system through various measures.<sup>75</sup> It controls monetary and other banking policies of the Indian government. The Reserve Bank was created by the Reserve Bank of India Act, 1934.<sup>76</sup>

“The function of Reserve Bank is specified in the Preamble of the RBI Act, 1934, it provides guidance to regulate the functioning of banks, they have provided the direction for circulating currency within the country.”<sup>77</sup> Under the provision of RBI, Act, 1934 RBI performs certain functions relating to Bank Notes' regulations; securing monetary stability managing the currency and credit system of India etc.<sup>78</sup>

A bank is to be called the Reserve Bank of India. The Central Government may, from time to time, give directions to the Banks after consultation with the Governor of the Bank.<sup>79</sup> The Bank shall be authorized to carry on and transact the several kinds of business, such as accepting money on deposit without interest from and collecting money from the Central Government, the State Government, local authorities, banks, and any other person. They can

---

<sup>74</sup> <https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20-Professional.pdf>

<sup>75</sup> Banking Law and Practice, 2014 URL: <https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20-Professional.pdf>

<sup>76</sup> <http://www.yourarticlelibrary.com/banking/reserve-bank/reserve-bank-of-india-originand-development/26356>

<sup>77</sup> Reserve Bank of India Functions. <https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20-Professional.pdf>

<sup>78</sup> Reserve Bank of India Act, 1934 URL: [https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018\\_FCD40172EE58946BAA647A765DC942BD5.PDF](https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018_FCD40172EE58946BAA647A765DC942BD5.PDF)

<sup>79</sup> Section 7(1) of RBI Act, 1934

also purchase, sale and rediscount of bills of exchange and promissory notes drawn on and payable in India and arising out of bona fide commercial or trade transactions bearing two or more good signatures, one of which shall be that of a scheduled bank (which is predominantly engaged in the acceptance or discounting of bills of exchange and promissory notes and which is approved by the bank).<sup>80</sup>

Suppose in the opinion of the Central Government the Bank fails to carry out any of the obligations imposed on it by or under the Act than it may by notification in the Gazette of India, declare the Central Board to be superseded and after that. In that case, the direction of the affairs of the Bank shall be entrusted to such an agency as the Central Government may determine. Such an agency may exercise the powers and do all acts and things that the Central Board may exercise as prescribed.<sup>81</sup>

RBI with the increase of users of internet banking services wants to provide a secure payment system to their customers so for electronic fund transfer and payment call for a committee in order to enact specific legislation which can provide protection to their customer's interest.<sup>82</sup> The Reserve Bank of India Act, 1934 was amended and electronic banking was included. Information Technology Amendment Act, 2008 as amended in the Reserve Bank of India Act 1934. Amendment has brought changes<sup>83</sup> by including laws for the

---

<sup>80</sup> Section 17 of RBI Act, 1934

<sup>81</sup> Section 30 of RBI Act, 1934: Power of Central Government to supersede Central Board.

<sup>82</sup> A committee headed by Shri S.R. Mittal was set up by RBI for Proposing Legislation on Electronic Fund Transfer and other Electronic. URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12_chapter%205.pdf)

<sup>83</sup> Section 58 of RBI Act: Power of the Central Board to make regulation- (1) The Central Board may, with the previous sanction of the [Central Government] [by notification in the official Gazette] make regulations consistent with this Act to provide for all matters for which provision is necessary or convenient for the purpose of giving effect to the provisions of this Act.

payment transaction between the different banks through electronic banking by using RTGS and NEFT and had mentioned the terms and conditions in order to complete the transaction among the banks and other financial

---

(2) In particular and without prejudice to the generality of the foregoing provision, such regulations may provide for all or any of the following matters, namely: -

(f) the manner in which the business of the Central Board shall be transacted, and the procedure to be followed at meetings thereof;

(g) the conduct of business of Local Boards and the delegation to such Boards of powers and functions;

(h) the delegation of powers and functions of the Central Board 1[\* \* \*] to Deputy Governors, Directors or officers of the Bank;

(i) the formation of Committees of the Central Board, the delegation of powers and functions of the Central Board to such Committees, and the conduct of business in such Committees;

(j) the constitution and management of staff and superannuation funds for the officers and servants of the Bank; (k) the manner and form in which contracts binding on the Bank may be executed;

(l) the provisions of an official seal of the Bank and the manner and effect of its use;

(m) the manner and form in which the balance-sheet of the Bank shall be drawn up, and in which the accounts shall be maintained;

(n) the remuneration of Directors of the Bank;

(o) the relations of the scheduled banks with the Bank and the returns to be submitted by the scheduled banks to the Bank;

(p) the regulation of clearing-houses for the banks 2(including post office savings banks).

[(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-I, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers.]

(q) the circumstances in which, and the conditions and limitations subject to which, the value of any lost, stolen, mutilated or imperfect currency note of the Government of India or bank note may be refunded; and 4

[(qa) the remuneration and other allowances payable to Members of the Monetary Policy Committee under sub-section (2) of section 45ZD;

(qb) the functions of the Secretary under sub-section (2) of section 45ZG;

(qc) the procedure, manner of conducting of meetings and related matters of the Monetary Policy Committee under sub-section (12) of section 45ZI

(qd) the particulars and the frequency of publication of document under sub-section (2) of section 45ZJ;

(qe) the form and contents of the Monetary Policy Report to be published under sub-section (2) of section 45ZM;] (r) generally, for the efficient conduct of the business of the Bank.

[(3) Any regulation made under this section shall have effect from such earlier or later date as may be specified in the regulation.

(4) Every regulation shall, as soon as may be after it is made by the Central Board, be forwarded to the Central Government and that Government shall cause a copy of the same to be laid before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation, or both Houses agree that the regulation should not be made, the regulation shall, thereafter, have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.]

[(5)] Copies of all regulations made under this section shall be available to the public on payment.

transactions.<sup>84</sup> “RBI encouraged India's electronic payment system through introducing different modes of payment system. They had already introduced and started using the same for the encouraging for the digital payment, such fund transfer are Electronic Clearing Service (ECS),<sup>85</sup> Electronic Fund Transfer (EFT), Real-Time Gross Settlement (RTGS), National Electronic Fund Transfer (NEFT) and Cheque Truncation System<sup>86</sup> (CTS).”<sup>87</sup>

The Working group was constituted in 2008 under the chairmanship of Shri. G. Gopalakrishna studied fraud that arises soon after the adoption of electronic banking. In the report, the committee shows the threats as a result of adoption of new banking service viz. electronic banking. Besides, the report enhances the importance of use of technology in order to identify anomalous e-banking transactions and enhancing audit processes using computer-assisted.<sup>88</sup> Reserve Bank is empowered to perform inspection or audit in banks under Banking Law Amendment Act, 2012. From time to time Reserve Bank of India is issuing guidelines and policy on electronic banking, information technology, and technology risk management for all commercial banks.<sup>89</sup>

---

<sup>84</sup> Clause (pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-I, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers. URL: <https://johnspaul7.blogspot.com/2019/03/st.html> (visited on 5.7.2018)

<sup>85</sup>Electronic Clearing Services (ECS) is an electronic mode of payment or receipt for the transaction. Institutions use it for making bulk payment amounts such as dividends, salary, pension, tax collection, insurance premium, and other receipts. URL: <https://www.rbi.org.in/commonman/Upload/English/FAQs/PDFs/ECS140311.pdf> (visited on: 5.7.2018)

<sup>86</sup>Cheque Truncation System (CTS) is a process of stopping the flow of the physical cheque issued by the drawer to the drawee branch and an electronic image of the cheque would be sent to the drawee branch along with the relevant information. URL: <https://m.rbi.org.in/Scripts/FAQView.aspx?Id=63> (visited on 5.7.2018)

<sup>87</sup> <http://www.legalserviceindia.com/legal/article-3322-e-banking-frauds-and-indianlegal-prospective.html>

<sup>88</sup>Gopalakrishna Committee on Cyber Frauds which recommended on Information Security, Electronic Banking, Technology Risk Management and Tackling Cyber Fraud.

<sup>89</sup> RBI Notification 2013-2014.

Reserve Bank of India is framing guidelines for all banks directing for the implementation process of internet banking.

Therefore, the Reserve Bank being regulatory of all banks will function as per the direction provided by RBI and all banking institutions having traditional and new delivery channels through internet facilities perform accordingly.

### **2.2.2. Banking Regulation Act, 1949:**

“The objective of the Banking Regulation Act, 1949 is to protect the interest of their customers. Banking regulation is a set of rules that act under the direction of the Reserve Bank to regulate bank functioning. It provides criteria to the banks for monetary and credit systems.<sup>90</sup> The RBI has exclusive power for the providing licence, they work as per their own discretion so it may issue, accept or reject any application for a licence to carry on banking business.<sup>91</sup>

The banking system made excellent achievements in the process of regulation of banking services of every possible means to their customers. Today banks are spread out in every corner of the country with new features added in their services. Till the 1990s Indian banking was operating in a traditional protected environment and soon after the adoption of LPG banking sectors entered into the intense competition. In order to perform smoothly banks have to protect the interest of the depositor and maintain public faith, they must have a fraud free system, adequate procedure and grievances remedial system. Banking has been defined by “Section 5(b) of Banking Regulation Act, 1949. Banking

---

<sup>90</sup> Banking Regulation Act, 1949

<sup>91</sup> Chapter 2: E-Banking URL:

<https://shodhganga.inflibnet.ac.in/bitstream/10603/89802/4/chapter%202.pdf>



means accepting deposits for the public which can be repayable on demand or can be withdrawal by cheques<sup>92</sup> or draft.”<sup>93</sup>

In the case of **Jawala Bank Ltd. vs. Shitla Parshad Singh**,<sup>94</sup> it was held that the definition of the Banking Company in the section does not mean that the company must, at the time in question, it must be able to accept deposits of money from the public which is repayable on public demand or on such terms which the money might have been deposited. It must mean that banking should be the primary business of the company even if, by reason of certain supervening cause, it is not able for the time being to carry on the work of receiving deposits and of making payments.

“Banking fraud is an act where a person intentionally forged the documents or temper bank’s computer system for the purpose of monetary gain.<sup>95</sup> Fraudulent transaction from the bank if occurred then the bank is under obligation to pay the loss of customer/depositor. If not then the bank has to prove and ensure that transaction has not been done fraudulently. In India, license has to be obtained from the Reserve bank of India under section

---

<sup>92</sup>Section 6 of Negotiable Instrument Act, 1881: A “Cheque” is a bill of exchange drawn on a specified banker and not expressed to be payable otherwise than on demand, and it includes the electronic image of a truncated cheque and a cheque in the electronic form.

- (a) “a cheque in the electronic form” means a cheque which contains the exact mirror image of a paper cheque, and is generated, written and signed in a secure system ensuring the minimum safety standards with the use of digital signature (with or without biometrics signature) and asymmetric cryptosystem;
- (b) “a truncated cheque” means a truncated cheque during the course of a clearing cycle, either by the clearinghouse or by the bank, whether paying or receiving payment immediately on the generation of electronic image transmission, substituting the further physical movement of the cheque in writing.

<sup>93</sup>Section 5(b) of the Banking Regulation Act, 1949 defines banking: Banking is the accepting deposits of money for the purpose of lending or investment from the public, repayable on demand or otherwise and withdrawal by cheque, draft, order, or otherwise.

<sup>94</sup> AIR 1950 AII 808

<sup>95</sup> [https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12_chapter%205.pdf)

22(1)<sup>96</sup> of the Banking Regulation Act for carrying on the banking business. Therefore, under section 49A of Banking Regulation Act, 1949, “no person other than a banking company or other banking institution or firm notified by the central government is only authorized to accept the deposits withdrawal by cheques.”<sup>97</sup>

The Banking Regulation Act, 1949, had been amended by Banking Laws (Amendment) Act, 2012, and it received presidential assent in January 2013. This amendment Act has created the way for issuing new banking licenses by giving greater responsibility of regulatory power to the Reserve Bank of India. The Banking Regulation Act has been amended by Banking Law Amendment Bill 2012.

The Amendment Bill of 2012 provides salient features to the Banking Law are as under:-

- a. The bill has given more power to direct the officials and bank management. RBI can exercise arbitrary power with consultation to the central government. It also provides RBI with the regulatory power to direct the boards of banks.
- b. The Reserve Bank of India can inspect the bank or other financial institution any time. They have the power to ask banks in order to

---

<sup>96</sup> Section 22(1) of Banking Regulation Act, 1949: Licensing of banking companies-(1) Save as hereinafter provided, no company shall carry on banking business in India unless it holds a licence issued in that behalf by the Reserve Bank and any such licence may be issued subject of such conditions as the Reserve Bank may think fit to impose.

<sup>97</sup> Section 49A of Banking Regulation Act, 1949: Restriction on acceptance of deposits withdrawable by cheque- No person other than a banking company, the Reserve Bank, the State Bank of India or any other [Banking institution, firm or other person notified by the Central Government in this behalf on the recommendation of the Reserve Bank] shall accept from the public deposits of money withdrawable by cheque. Provided that nothing contained in this section shall apply to any savings bank scheme run by the Government.

check bank records, inspect books so that they can prevent or stop the improper banking management which can cause greater loss in future.

- c. Amendment bill has increased voting rights in any company or bank. RBI has given the power for accepting the proposal and this is all done with the motive to place the financial institution or company in the hand of a good person.<sup>98</sup>

### 2.2.3. Indian Contract Act, 1872:

Indian Contract Act is one of the oldest Act of India. It ensures parties with the rights and obligations which arise out of a legal contract. To make a Contract<sup>99</sup> valid there they must fulfill the specific requirements for lawful consideration.<sup>100</sup> The parties entering into the contract must be competent<sup>101</sup> enough to understand the necessity and requirements of the contract. The Indian contract Act had already mentioned the condition for a valid contract. The parties to the contract must be major and of sound mind where the consent for the contract can't be obtained under any influence<sup>102</sup> and must be a valid contracts to be enforceable.

---

<sup>98</sup> URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12_chapter%205.pdf)

<sup>99</sup>Section 10 of Indian Contract Act 1872: All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object and are not hereby expressly declared to be void.

<sup>100</sup> Section 2 (d) of the Indian Contract Act 1872: Consideration means a reasonable equivalent or other valuable benefit passed on by the promisor to the promisee.

<sup>101</sup>Section 11 of Indian Contract Act, 1872: Who are competent to contract- Every person is competent to contract who is of the age of majority according to the law to which he is subject, and who is of sound mind, and is not disqualified from contracting by any law to which he is subject.

<sup>102</sup> Section 12 of Indian Contract Act 1872: A person is said to be of sound mind to make a contract, if, at the time when he makes it, he is capable of understanding it and of forming a rational judgment as to its effect upon his interests.

A person, who is usually of unsound mind, but occasionally of sound mind, may make a contract when he is of sound mind. A person, who is usually of sound mind, but sometimes of unsound mind, may not make a contract when he is of unsound mind.

“The formation of traditional contracts in offline mode has already been settled. On the internet the regulation of traditional contracts may not be equally applicable to the world of cyberspace in cyberspace. E-contract<sup>103</sup> is a form of contract created using an electronic system which is born out of the need of the people for speed, suitability, and efficiency.”<sup>104</sup> An E-contract is a contract that is formed in e-commerce<sup>105</sup> by the two or more parties using electronic means.<sup>106</sup> Unlike traditional contracts, e-contract will only be completed after fixing digital signatures<sup>107</sup> in contract paper. Thereafter it will be valid and binding to both the parties. “Like every other traditional contract, it also requires some specific requirements for making it a valid contract for lawful consideration. Similar to other contracts the e-contract also requires an offer to be made<sup>108</sup> and acceptance must be made.”<sup>109</sup>

As per traditional principle of Indian Contract Law, the acceptance of contract may be expressed in writing or oral and the time of acceptance is based on the

---

Section 13 of the Indian Contract Act, 1872: “Consent” means “two or more persons are said to consent when they agree upon the same thing in the same sense.”

Section 14 of Indian Contract Act, 1872: Consent is said to be free when it is not caused by (1) coercion, as defined in section 15, or (2) undue influence, as defined in section 16, or (13) fraud as defined in section 17 or (4) misrepresentation, as defined in section 18 or (5) mistake

Section 16 of Indian Contract Act, 1872: A contract is said to be induced by “undue influence” where the relations subsisting between the parties are such that one of the parties is in a position to dominate the will of the other and uses that position to obtain an unfair advantage over the other.

<sup>103</sup> Section 10 of Indian Contract Act 1872: What agreements are contracts: All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void. Nothing herein contained shall affect any law in force in India, and not hereby expressly repealed, by which contract is required to be made in writing or in the presence of witnesses, or any law relating to the registration of documents.

<sup>104</sup> Ranka Shreyans, “All About E-contracts- Meaning, Types and Law”, 2015 available at <https://taxguru.in/corporate-law/all-about-e-contracts-meaning-types-and-law.html>

<sup>105</sup> Section 2(16) of Consumer Protection Act 2019: “e-consumer” means buying or selling of goods or services including digital products over digital or electronic networks.

<sup>106</sup> Definition provided by U.S “The Uniform Computer Information Transactions Act.”

<sup>107</sup> Section 2(1)p of IT Act, 2000: Digital Signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

<sup>108</sup> In e-contract offers for the contract are not made directly, and the offer is made by the customer on introduction of the products.

<sup>109</sup> <https://taxguru.in/corporate-law/all-about-e-contracts-meaning-types-and-law.html>

parties whether they wanted to meet physically or sign it in different places. The communication of proposals complete against the offeree only when it comes to his knowledge of the person against whom such proposal is made.<sup>110</sup> Whereas in the internet various means of communication for acceptance and offer can be used by the parties such as emails, messenger or through any other act that indicates acceptance of the offer. Section 12<sup>111</sup> of the Information Technology Act, 2000 the acceptance will be binding on the receipt of an acknowledgement of an electronic record on the offeree, when acceptance moves out of the control of the offeree it shall be binding on the offeror on receiving the acceptance. Section 12(2) there is proper means of acknowledgement stipulated by the parties. If such acknowledgement is not

---

<sup>110</sup> Section 4 of Indian Contract Act, 1872: Communication when complete- The communication of a proposal is complete when it comes to the knowledge of the person to whom it is made.

The communication of an acceptance is complete-

as against the proposer, when it is put in a course of transmission to him, so as to be out of the power of the acceptor;

as against the acceptor, when it comes to the knowledge of the proposer.

The communication of a revocation is complete,—

as against the person who makes it, when it is put into a course of transmission to the person to whom it is made, so as to be out of the power of the person who makes it;

as against the person to whom it is made, when it comes to his knowledge.

Illustrations: (a) A proposes, by letter, to sell a house to B at a certain price. The communication of the proposal is complete when B receives the letter.

(b) B accepts A's proposal by a letter sent by post. The communication of the acceptance is complete, as against A when the letter is posted; as against B, when the letter is received by A.

(c) A revokes his proposal by telegram. The revocation is complete as against A when the telegram is despatched. It is complete as against B when B receives it. B revokes his acceptance by telegram. B's revocation is complete as against B when the telegram is despatched, and as against A when it reaches him

<sup>111</sup>Section 12 of Information Technology Act, 2000: Acknowledgement of receipt- (1) Where the originator has not [stipulated] that he acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by-

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator

(3) Where the originator has stipulated that electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

received as stipulated by the parties than the electronic record shall not be binding, thus acknowledgment is must for a binding contract.

Now the question arises, where the contract is formed in Cyberspace? As per the Indian Contract Act, a traditional contract is completed on the time when the offeree makes a declaration of acceptance saying that he has accepted the offer or contract is completed on the dispatch of letter which contains the letter of offer. In case of **Entores Ltd. v. Miles Far East Corpn.**,<sup>112</sup> offer was made in Amsterdam and the acceptance was received in London, the court held that in case of instantaneous communication the contract shall be formed where it is received the acceptance. Indian Court followed the same principle of Common Law in the case of **Bhagwandas Goverdhandas Kedia v. M/S. Girdharilal Parshottamdas.**<sup>113</sup> The case is very important in the history as an Act of 1872 cannot have principles of technology. Thus interpreting a law (precedent) in the light of advanced technology has historical importance.

Indian Contract Act defined Fraud under section 17<sup>114</sup> of the Indian Contract Act. The section contains certain elements to constitute fraud which includes false statement of fact with a dis-belief of its truthfulness. This statement should be made with a wrongful intention to deceive and thereby inducing the person to enter into the contract on that basis.”<sup>115</sup> Fraud committed on the

---

<sup>112</sup>Entores Ltd. v. Miles Far East Corpn., (1955) 2 QB 327

<sup>113</sup> 1966 AIR 543, 1966SCR (1) 656

<sup>114</sup> Fraud means and includes any of the acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him, to enter into the contract:

- 1). The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
- 2). The active concealment of a fact by one having knowledge or belief of the fact;
- 3). A promise made without any intention of performing it;
- 4). Any other act fitted to deceive;
- 5). Any such act or omission as the law specially declares to be fraudulent.

<sup>115</sup> R. K. Bangia, “*Indian Contract*”, 6<sup>th</sup> Edition 2009, Allahabad Law Agency

bank is a criminal act whose intention was to make financial gain or benefit, and the definition of fraud stated under the Indian Contract Act can be used to know the meaning and for claiming compensation for the loss occurred by committing such act.

#### **2.2.4. Indian Penal Code, 1860:**

Indian Penal Code, 1860, is an important penal law prevailing in India and it is used for penalizing the accused for their criminal act. It covers almost all the substantive aspects of criminal laws.<sup>116</sup> In developing countries with the adoption of advancement in technology, there has been a rapid growth of cyber fraud. The reason for the growth of digital crime is due to the fast flow of the internet and its digitized activities. The improvements in banking technologies are creating customer convenience which has resulted in the rise of cyber criminals to commit cyber fraud. Indian Penal Code has not mentioned any definition or punishment for cyber fraud. So generally, cyber fraud is an act of deception for securing the personal banking details with the help of computers and the internet. In order to understand cyber fraud, we need to understand similar offence relating to cyber fraud they are cheating (Section 415), dishonestly (Section 24), and fraudulently (Section 25).

As we all know, cheating is a criminal offence, and it can be seen in various forms. Generally, cheating can be described as a dishonest or unfair act done to gain profit over another. Cheating is an act of saying or doing something dishonestly about something which is not valid in the eyes of law. Cheating it

---

<sup>116</sup> Indian Penal Code, 1860 also see: [Cyber\\_Crime\\_Law\\_and\\_Practice.pdf \(icsi.edu\)](#)

has been defined under section 415<sup>117</sup> of IPC, 1860, and to consider the offence as cheating, there must be essential elements such as deception and inducement.<sup>118</sup> In cheating, deceiving<sup>119</sup> is the important part of the offences but all deceptions does not amount to cheating. Deception done intentionally, dishonestly, fraudulently will consider to be cheating<sup>120</sup> and whoever cheats with wrong intention shall be punished under section 415 of IPC.<sup>121</sup>

Similarly, “Dishonestly” has been defined under section 24 of IPC<sup>122</sup> where people intentionally cause wrongful loss to another person. As per section 25 person intending to act fraudulently try to defraud another person.<sup>123</sup> It has merely said there could be no fraud unless there was an intention to defraud. Thus, here it makes intention as the genesis of fraud, whereas in the contract law, fraud is clearly defined.

According to Section 17 of Indian Contract Act 1872, Fraud means any person who intentionally entered into the contract in order to deceive other parties in

---

<sup>117</sup>Section 415 of Indian Penal Code, 1860: 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 intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat"

<sup>118</sup>Section 420 of Indian Penal Code, 1860- Cheating and dishonestly inducing delivery of property.—Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

<sup>119</sup>Deceiving means causing to believe what is false or misleading as a matter of fact. See: <https://blog.ipleaders.in/cheating-fraud/>

<sup>120</sup>Anubhav Pandey, " Indian Penal Code on Fraud and Cheating" posted on 11th April 2017 available at <https://blog.ipleaders.in/cheating-fraud/> visited on 1/03/2019

<sup>121</sup>Section 415 IPC “Whoever cheats shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.”

<sup>122</sup>Section 24 of Indian Penal Code, 1860: Dishonestly- whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person is said to do that thing dishonestly.

<sup>123</sup>Section 25 of Indian Penal Code, 1860: fraudulently- “A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.”



order to gain profit over others.<sup>124</sup> Fraud means an intention to deceive, whether from any expectation of advantage to the party himself or the ill will towards the other. Thus for proving the ‘fraud’ two essential ingredients must be present use of deceitful means and injury to the person so deceived the act.<sup>125</sup>

IPC has been amended by the Information Technology Act, 2000 (amended act 2008). The IT Act, has inserted offences related to electronics under Indian Penal Code. With amendment Act 2000 electronic documents which are stored in computer systems are made admissible as electronic.<sup>126</sup> IPC penalizes certain cybercrimes such as cyber fraud or tampering the digital evidences etc.”<sup>127</sup> Although there is no proper definition of cyber fraud or internet fraud, the courts in India have dealt with many e-banking fraud cases by combining several sections of IPC and IT Act. The investigating and prosecuting authorities faces difficulty in treating different crimes under same provisions of laws but a combined reading of information technology with Indian Penal Code makes the task of investigating and prosecuting quite easy.

---

<sup>124</sup>Section 17 of Indian Contract Act, 1872: “Fraud” defined- “Fraud” means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent<sup>2</sup>, with intent to deceive another party thereto of his agent, or to induce him to enter into the contract:-

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

Explanation.—Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak<sup>3</sup>, or unless his silence is, in itself, equivalent to speech.

<sup>125</sup> State of Andhra Pradesh v. T. Suryachandra Rao, AIR 2005 S.C. 3110

<sup>126</sup>[https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12_chapter%205.pdf)

<sup>127</sup> [http://nja.gov.in/Concluded\\_Programmes/2018-19/P-1125\\_PPTs/6.Electronic%20Evidence-%20Collection%20Preservation%20and%20Appreciation.pdf](http://nja.gov.in/Concluded_Programmes/2018-19/P-1125_PPTs/6.Electronic%20Evidence-%20Collection%20Preservation%20and%20Appreciation.pdf)

### 2.2.5. Indian Evidence Act, 1872:

The Indian Evidence Act's adoption changed the entire system of concept pertaining to the admissibility of evidence before the Indian court. The fragile nature of evidence in the virtual world is very complex to deal with so it's totally different, and they generally gather the evidence in the form of fingerprints, weapons of crime, bloodstain marks, submitted to the court. The definition of "evidence" provided by Indian Evidence Act 1872 includes oral evidence and all the documents including electronic records.<sup>128</sup> In **Anvar P.V v. P. K. Basheer, on 18 September 2014**,<sup>129</sup> Lordship observed that Information Communication Technology had a greater impact in human life. This changed the perception of doing business as it brought complete transaction. Adoption of Information technology has similarly brought changes in judiciary by introducing electronic evidence. Even in the judiciary technology has made a positive impact. If it is properly guided then it makes the system to function faster and in an effective way. The Supreme Court held that for any evidence to be admissible before the court it must meet the necessary requirements of Section 65B, which includes giving certificate as per Section 65B(4).

In **State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru**,<sup>130</sup> the Supreme Court states that the only option to prove the electronic evidence is

---

<sup>128</sup>Section 3 of Indian Evidence Act, 1872: Evidence- "Evidence" means and includes- (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry;  
such statements are called oral evidence;

(2) [all documents including electronic records produced for the inspection of the Court;] such

documents are called documentary evidence.

<sup>129</sup> (2014) 10 SCC 437

<sup>130</sup> (2005) 11 SCC 600

by producing original electronic media as the primary evidence or by secondary evidence under Section 65A and 65B of Evidence Act and it must be accompanied with a certificate without which electronic evidence will be inadmissible before the court.

Cybercrime is a faceless crime, conducted using internet and computer technology as a tool or computer as a target. In such cases, it is very problematic to collect evidence, since cybercrime evidence lies within the understanding of the modus operandi of a cyber fraud and must be an efficient knowledgeable computer forensics expert. The Indian Evidence Act has recognized expressions such as Certifying Authority,<sup>131</sup> Electronic Signature,<sup>132</sup> Electronic Signature Certificate,<sup>133</sup> electronic form, electronic records,<sup>134</sup> information,<sup>135</sup> secure electronic record, and the secure digital signature<sup>136</sup> as defined under the information Technology Act, 2000.<sup>137</sup> Till 2000, electronic evidence had no recognition under the law. Under Section 17 word for ‘oral or documentary’ was substituted by oral or documentary or

---

<sup>131</sup> Section 2(1)(g) of IT Act 2000 “Certifying Authority” means a person who has been granted a licence to issue a Digital Signature Certificate under section 24.

<sup>132</sup> Section 2(1)(ta) of IT Act 2000 "Electronic Signature" means authentication of any electronic records by the subscriber through the electronic technique specified in Second Scheduled and includes a digital signature

<sup>133</sup> Section 2(1)(tb) of IT Act 2000 “Electronic Signature Certificate” means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate.

<sup>134</sup> Section 2(1)(t) "Electronic Records" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche.

<sup>135</sup> Section 2(1)(v) of IT Act 2000: “Information” includes [data, message, text] images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche

<sup>136</sup> Section 2(1)(p) of IT Act, 2000: “digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3

<sup>137</sup> Section 3 of Indian Evidence Act, 1872

contained in electronic form<sup>138</sup> and the word 'record' was substituted by word 'record or by electronic record'.<sup>139</sup>

Section 65<sup>140</sup> was amended and two sections 65A<sup>141</sup> and 65B<sup>142</sup> were added to the Indian Evidence Act, 1872, by the IT Amendment Act 2008. The inclusion

---

<sup>138</sup> Substituted by Act 21 of 2000

<sup>139</sup> Section 35 of Indian Evidence Act 1872: Relevancy of entry in public [record or an electronic record] made in the performance of duty- An entry in any public or other official book, register or [record or an electronic record], stating a fact in issue or relevant fact, and made by a public servant in the discharge of his official duty, or by any other person in the performance of a duty specially enjoined by the law of the country in which such book, register, or [record or an electronic record] is kept, is itself a relevant fact

<sup>140</sup> Section 65 of Information Technology Act 2000: Tampering with Computer Source Documents- Whoever knowingly or intentionally conceals, destroy or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with the fine which may extend upto two lakh rupees, or with both.

<sup>141</sup> Section 65A of Indian Evidence Act 1872: Special provisions as to evidence relating to the electronic record.

<sup>142</sup> Section 65B of the Indian Evidence Act 1872: Admissibility of electronic records- (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:-

- (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
- (b) during the said period, information of the kind contained in the electronic record or of the kind from so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
- (c) 'throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
- (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether-

- (a) by a combination of computers operating over that period; or
- (b) by different computers operating in succession over that period; or
- (c) by different combinations of computers operating in succession over that period, or
- (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as

of those sections gives legal recognition to electronic records and considers them as authenticated documents that are admissible in the court. The Delhi High Court in the case of **Societe Des Products Nestle S. A and Anr vs. Essar Industries and Ors**<sup>143</sup> paved way for the immediate introduction of Section 65A and 65B in the Indian Evidence Act, 1872 relating to the admissibility of the computer generated in a practical way to eliminate the challenges to electronic evidence. According to Section 65A the content of the electronic records can be proved by parties as per the direction issued by certifying authority with section 65B of the Indian Evidence Act, 1872 and electronic records are admissible as evidence before court.<sup>144</sup>

---

constituting a single computer; and references in the section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-

- (a) identifying the electronic record containing the statement and describing the manner in which it was produced;
- (b) giving such particulars of any device involved in the production of the electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
- (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a maker to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

- (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
- (b) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
- (c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation- For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.]

<sup>143</sup> 2006 (33) PTC 469 Del

<sup>144</sup> 2003 VIIAD Delhi 1, 107 (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669

Similarly, various other amendments were such as proof as to verification of the digital signature,<sup>145</sup> the presumption as to digital signature certificate,<sup>146</sup> before the court.<sup>147</sup> The Indian Evidence Act also addresses the issues of electronic evidence. “Electronic evidence is documents that are stored in a computer system that are collected after the investigation in such a form that can be produced in the court.”<sup>148</sup> Since electronic evidence is invisible where it can be altered or destroyed easily, to deal with the cyber offences for collecting evidence one needs special training and proper equipped tools.<sup>149</sup> Thus, electronic records admissibility as evidence stated under section 65B in the Indian Evidence Act covers almost all types of electronic records as evidence.

#### **2.2.6. Information Technology Act, 2000:**

The rapid growth of information technology made everyone dependent on technology which had a great impact over every individual. These technologies made possible transformations from traditional banking to digital banking. Most of the impact of advanced technology has been seen on the banking sector. The users of computers and the internet are increasing, so do the cyber criminals are also creating new modus operandi for misusing the computer and internet for their malicious motive. Agencies for dealing cyber fraud should be strong minded people who are knowledgeable enough to use

---

<sup>145</sup> Section 73A of Indian Evidence Act: Proof as to verification of digital signature.

<sup>146</sup> Section 85c of Indian Evidence Act

<sup>147</sup> Section 131of Indian Evidence Act: Production of documents or electronic records which another person, having possession, could refuse to produce.

<sup>148</sup> *Supra* note at 128

<sup>149</sup> Dr. S Murugan, “Electronic Evidence: Collection, Preservation and Appreciation”, URL: [http://nja.gov.in/Concluded\\_Programmes/2018-19/P-1125\\_PPTs/6.Electronic%20Evidence-%20Collection%20Preservation%20and%20Appreciation.pdf](http://nja.gov.in/Concluded_Programmes/2018-19/P-1125_PPTs/6.Electronic%20Evidence-%20Collection%20Preservation%20and%20Appreciation.pdf) (visited on 22.7.2018)

the computer technology for investigation. If possible they must acquire subject knowledge of computer forensics that can play with the codes or encryption or binary digits.<sup>150</sup> Growth of electronic commerce eliminates paper transactions, and encourages electronic payment systems. Information Technology Act has been framed as per the Model Law on Electronic Commerce, 1996. Considering the needs for the regulation of electronic governance and e-commerce, the bill for Information Technology was passed.<sup>151</sup> By adopting Information Technology India became the 12th country who passed cyber law to deal with cybercrime or offences. The Act gives a new transformation shift in legal enforcement as it introduces electronics as a new medium of producing, using and presenting evidence in the 21st century.”<sup>152</sup> Electronic evidence has been admissible in the court of law by virtue of amendment made in the Indian Evidence Act. The Information technology Act brought these amendments to the evidence law.

The Information Technology Act, 2000, is considered as the cyber law of India as it deals with all the offences related to computers and the internet. It even made electronic evidence admissible in Indian court as it is equivalent to traditional evidence. Unfortunately, this Act failed to mention cyber fraud in the whole of Information Technology Act 2000. There is no suction that mentions or talks about the definition or punishment for cyber fraud. No specified definition of cyber fraud is provided. The IT Act, 2000 covers every aspect of cyber crime as it is the Cyber Law of India. It is creating difficulties

---

<sup>150</sup>Law relating to cybercrime in India URL: [http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08\\_chapter%203.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08_chapter%203.pdf) (visited on 2.9.2018)

<sup>151</sup> The Information Technology Act, 2000

<sup>152</sup>The Preamble of IT Act, 2000 provides that the Act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce.

before investigating officers and the judiciary while pronouncing verdict for cyber fraud. While IT Act 2000 previously had only two sections i.e. section 43<sup>153</sup> and 60<sup>154</sup> dealing with computer-related offences generally. To understand the concept of cyber fraud one needs to go through the different definitions of terms that are related to computers. IT Act, 2000 defines the term access in Section 2(1) (a),<sup>155</sup> computer network in Section 2(1)(j),<sup>156</sup> Computer in Section 2(1)(i),<sup>157</sup> data in Section 2(1)(o),<sup>158</sup> and information in

---

<sup>153</sup> Section 43 of IT Act, 2000(before amendment Act 2008): If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,- (a) accesses or secure access to such computer, computer system or computer network; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

<sup>154</sup>Section 60 of IT Act, 2000(before amendment act 2008): the provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

<sup>155</sup> Section 2(a) of IT Act, 2000 “ access”, With its grammatical variation and cognate expression, means gaining entry into instructing or communicating with the logical, arithmetical or memory functions resources of a computer, computer system or computer network.

<sup>156</sup> Section 2(j) “Computer network” means the inter-connection of one or more computers or computer system or communication device through-(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media and (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained.

<sup>157</sup> Section 2(i) “Computer” means any electronic, magnetic, optical or other high speed data processing device or system which perform logical, arithmetic or optical impulses, and includes all inputs, outputs, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

<sup>158</sup> Section 2(o) “Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.



Section 2(1)(v).<sup>159</sup> These are all the necessary ingredients that are useful to technically understand the concept of cyber fraud.

IT Act, 2000 focuses on providing recognition of transactions using electronic payment systems. The Act encourages the electronic payment system and supports digital governance by allowing the documentation by online mode in digital format. They have also updated the laws and have tried to create laws for cyber crime through amendment act 2008.<sup>160</sup> Since the growth of cyber fraud is growing with the growth of technology. To combat cyber crime in the world they amended the IT Act, 2000 by amendment act 2008.

Digitalization of banking services had made a convenient process as it provides every banking service online to customers but along with it, there is arising a question related to cyber security.<sup>161</sup> While opening an account in the bank one has to give every personal detail, similarly in internet banking also we display our details in the computer system which will be stored there in the system. Hackers can easily manipulate the system so that they can obtain bank details.

In order to help national incidence, Indian Computer Emergency Response Team (CERT-In) has been established as an agency of the government. CERT-In has been operational since January, 2004. CERT-In as a functional organization of the MEITY, Government of India is established to secure

---

<sup>159</sup> Section 2(v) “Information” includes [data, message, text], images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche.

<sup>160</sup> Aastha Bhardwaj, Priyanka Gupta, “ IT Act 2000: Scope, Impact And Amendments”, International Journal of Electrical Electronics & Computer Science Engineering, ISSN: 2348-2273, 2015

<sup>161</sup>Section 2(nb) of IT Act 2000: “Cyber Security” means protecting information, equipment, devices, computer, computer resources, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

Indian cyber space.<sup>162</sup> CERT-In as a single authority holds power to block any websites if contains contents in violation of any law in force.<sup>163</sup>

The prime objective of CERT-In are:-

- a. Preventing cyber attacks against the country's cyber space.
- b. Responding to cyber attacks and minimizing damage and recovery time Reducing 'national vulnerability to cyber attacks
- c. Enhancing security awareness among common citizens.

Indian Computer Response Team-In as designated by the Information Technology (Amendment) Act 2008, working as nodal agency helping government issues related to cyber security:-<sup>164</sup>

---

<sup>162</sup> <https://cert-in.org.in/>

<sup>163</sup> Section 70B of IT Act 2000: Indian Computer Emergency Response Team to serve as national agency for incident response-(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

(4) the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,-

- (a) collection, analysis and dissemination of information on cyber incidents;
- (b) forecast and alerts of cyber security incidents;
- (c) emergency measures for handling cyber security incidents;
- (d) coordination of cyber incidents response activities;
- (e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- (f) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be as such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person.

(7) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1).

<sup>164</sup> Indian Computer Emergency Response Team Ministry of Electronics and Information Technology Government of India, URL: <https://cert-in.org.in/>

- a. They collect the records of incidents of cyber crime and analyze the data to check the growth rate of the incident and try to stop the crime if possible.
- b. After collecting the information of the cyber crime they will direct the authority to look into the matter and send alerts of cyber crime if they traced the incident beforehand.
- c. They provide to the government or institution for the security measures that they can follow in case of emergency cyber incidents.
- d. The agency creates a coordination of incidents and issues different guidelines or advisory notes for reporting or for the security practice procedure to be followed in case of cyber emergency.
- e. They perform such other functions related to cyber security as prescribed.

According to section 43 of IT Act, 2000 if any tries to tamper computer information or damage or alter or change any information in computer system fraudulently will be punished under section 43.<sup>165</sup> If anyone neglects to

---

<sup>165</sup> Section 43 of IT Act, 2000:[Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,—

- (a) accesses or secures access to such computer, computer system or computer network[or computer resource];
- (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
- (e) disrupts or causes disruption of any computer, computer system or computer network;
- (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
- (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

perform their duty of security practices as prescribed under section 43 will be held liable for the offence and punished accordingly as prescribed.<sup>166</sup> Banks and financial institutions are dealing with the technology which is at the risk of being fraud. They are trying to upgrade their security system to protect the customer interest. If any corporate fails to provide their service of security, or lie deficiency in their service will be liable.<sup>167</sup>

If anyone retains the stolen computer property will be punished under section 66B of information Technology Act.<sup>168</sup> Cyber fraud has become a great threat

---

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

[(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]

2[he shall be liable to pay damages by way of compensation to the person so affected.]

Explanation.—For the purposes of this section,—

(i) —computer contaminant means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) —computer data-base means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) —computer virus means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) —damage means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

[(v) —computer source code means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]

<sup>166</sup> Section 66 of IT Act, 2000: Computer related offences- If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both

Explanation.—For the purposes of this section,— (a) the word —dishonestly shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860); (b) the word —fraudulently shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

<sup>167</sup> Section 43A of IT Act, 2000: Compensation for failure to protect data- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing reasonable security practices and procedure and thereby cause wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

<sup>168</sup>Section 66B of IT Act 2000: Punishment for dishonestly receiving stolen computer resource or communication device- Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or

to everyone all over the world. There is no specific department that looks after cyber fraud. In India the investigation powers are provided by the legislature to the Sub-Inspector.<sup>169</sup>

### **2.2.7. National Cyber Security Policy, 2013:**

National Cyber Security Policy, 2013 was formulated to create a secure cyber ecosystem in the country so that it can generate adequate trust and confidence in IT systems and transactions in cyberspace. The IT sector has emerged as one of the most significant sectors for the growth of Indian economy. This sector played a vital role in transforming Indian banking system. The Cyber security policy is a guideline to provide security practice which is to be applied in emergency cases of cyber incidents. The policy helps in securing the sensitive information which is there in cyberspace. They issue guidelines from time to time in order to protect the customer interest and their information.”<sup>170</sup>

National Cyber Security Policy was set up with objectives<sup>171</sup> of establishing a secure cyber ecosystem. This was basically with the aim of developing trust and confidence of public in IT systems and thus to increase the electronic transactions. The whole idea behind this policy was to increase cyber adoption

---

communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

<sup>169</sup>Section 80 of Cr. P. C. 1973: Procedure on arrest of person against whom warrant issued- When a warrant of arrest is executed outside the district in which it was issued, the person arrested shall, unless the Court which issued the warrant is within thirty kilometres of the place of arrest or is nearer than the Executive Magistrate or District Superintendent of Police or Commissioner of Police within the local limits of whose jurisdiction the arrest was made, or unless security is taken under section 71, be taken before such Magistrate or District Superintendent or Commissioner

<sup>170</sup> Ministry of Communication and Information Technology National Cyber Security Policy, 2013, Department of Electronics and Information Technology URL: [https://nciipc.gov.in/documents/National\\_Cyber\\_Security\\_Policy-2013.pdf](https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf)

<sup>171</sup>National Cyber Security Policy, 2013: Objectives [https://nciipc.gov.in/documents/National\\_Cyber\\_Security\\_Policy-2013.pdf](https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf)

of promote digitalization. The policy also aimed to bring compliance to global security standards.

The policy with Information Technology Act was an addition to the Indian cyber regulatory framework. Thus this policy was introduced to be more vigilant and attentive towards the cyber-attacks. And it was expected that policy will enhance national and sectorial level mechanism which will be able to get more strategic information regarding threats to ICT infrastructure. This information may help getting them to be prepared and effective in handling the threats.

The policy was designed to not only enhance the protection but also resilience of Nation's critical information infrastructure. The Policy aimed at providing appropriate indigenous security and to improve visibility of the integrity of ICT products and services. They aimed to introduce with a huge workforce of skilled professionals. Fiscal benefits to businesses were also one of the objectives that policy aimed. Citizen's privacy, data theft, effective prevention, proper investigation and then prosecution of cybercrime were major challenges that policy discussed. The policy also deliberated upon law enforcement capabilities and requirement of appropriate legislative intervention.

The major emphasis is on policy guidelines about developing effective public private partnerships (PPP). An emphasis is also supplied on; collaborative engagements. The policy also emphasized on mutual cooperation and understating amongst nations for furthering the cause of security of cyberspace through technical and operational cooperation

India after having a number of policies they are still unable to combat the challenges of cybercrime as a whole. 2013 policy is also trying to strengthen the regulatory framework addressing technology challenges that are changing with the development of technology along time. It has also provided guidelines to all the IT companies, banks, financial institutions and among the public in general about creating cyber security awareness with the different modes and methods. They can organize seminars and workshops about cyber security in which electronic media can be used for obtaining great benefits. But the changing nature of cyber threats has been challenging the regulators, judiciary, and researchers to look over the existing laws and it clearly shows the need for new laws.

Since India is going through a digital revolution there is a need for a new cyber policy.<sup>172</sup> Even Prime Minister Narendra Modi, in his Independence Day 2020 speech, said that his government is aware of the threats arising from cyberspace and their potential impact to India's society, economy and development; he also announced that India will soon have a new cyber security policy.<sup>173</sup> With the advent of time there has been a rise not only in cases of cyber fraud but also in cybercrime cases as a whole along with new methods and techniques of conducting the crimes.

### **2.3. Legal and Regulatory structure of European Banking Industries:**

This section provides important legislation affecting the regulation of banks in the European Union (EU). The global banking system had experienced some substantial

---

<sup>172</sup> Ravi Shankar Prasad, Minister for Information and Technology told India Today dated: 15<sup>th</sup> August, 2020

<sup>173</sup> India Today Dated: August 16, 2020

crisis and instead of this, the European banking system has shown some remarkable developments. It has increased its bank's financial strength and even improved risk management techniques. Banks in the EU are making more efforts to cut costs and developing internet banking is one of the ways to improve cost.<sup>174</sup> Internet banking adopted a new process of providing their services using online tools.<sup>175</sup> The internet banking is predominantly being used for basic deposit based transactions and for buying goods and services.<sup>176</sup> After the crisis of 2008, the "major banks in the EU have invested in providing internet banking services as new cost-effective delivery channels. Thus, e-banking includes automated teller machines (ATM), telephone banking, mobile banking, digital television, debit and credit cards, internet banking, etc., became one of the main battlefields of the banking industry."<sup>177</sup>

The European Union banking regulation and supervision is not a creation of recent year discussion. The development in EU legislation has taken place against the crisis since 2011, concerning the eurozone banks and threats to financial stability in the EU. All the Member States of the EU are bounded by the regulation of banks that have taken the form of EU regulations. Recently the European supervisory and European Commission has introduced a 'Single Rule Book' for financial services in the EU. In EU banking three main elements are nested under the umbrella term of "banking

---

<sup>174</sup>European Central Bank: Structural Analysis of The EU Banking Sector November 2002 available at <http://www.ecb.int>

<sup>175</sup> European Commission Report 2005 [http://www.ub.edu/irea/working\\_papers/2008/200811.pdf](http://www.ub.edu/irea/working_papers/2008/200811.pdf)

<sup>176</sup>Arnaboldi Francesca and Claeys Peter, "*Internet Banking in Europe: a comparative analysis*", Research Institute of Applied Economics 2008 URL: [http://www.ub.edu/irea/working\\_papers/2008/200811.pdf](http://www.ub.edu/irea/working_papers/2008/200811.pdf)

<sup>177</sup>AtayErhan&ApakSudi, "*An overview of GDP and internet banking relations in the European Union versus China*", Procedia- Social and Behavioral Sciences 2013 URL: <https://core.ac.uk/download/pdf/81163576.pdf> (visited on 10.2.2019)



union” i.e., regulation (single rulebook), supervision (single supervisory mechanism or SSM,) and resolution (single resolution mechanism or SRM).<sup>178</sup>

Information technology is fundamentally changing the scenario of the banking industry. European banks have leveraged internet banking for cross-border expansion, consolidation, and competition. However, e-banking in the European Union with a single currency raises regulatory and technical issues.<sup>179</sup> Today banks are offering internet banking since its cost-effectiveness and increased customer reach. Internet banking is currently offered by most of the banks throughout the EU. If it is done appropriately than online banking improves customer satisfaction, improves profitability and it also brings competition among bank’s policies and services for consumers.<sup>180</sup> Finally, internet banking could be an enabling instrument for cross-border bank expansion. Bank took several changes to establish internet banking which will extend improvements in banking services for consumers.<sup>181</sup>

European banks and financial services regulatory authorities are stepping up cooperation to make retail payments safer. Increasingly frequent and highly sophisticated cyber-attacks continue to permeate every pathway that crosses the digital landscape. Evolving security threats and advanced technologies are subjecting internet commerce to significantly higher rates of fraud than traditional payment methods. Banks and other service providers face an urgent need to deploy more

---

<sup>178</sup>Mourlon- Druol Emmanuel, “ *Banking Union in Historical Perspective: The Initiative of the European Commission in the 1960s-1970*”, Journal of Common Market Studies 2016 Vol.54 URL: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/jcms.12348>

<sup>179</sup>Pyun, Chong Soo; Scruggs, Les; Nam, Kiseok, “ *Internet Banking in the U.S., Japan and Europe*”, Multinational Business Review, Fall 202 URL: <https://www.questia.com/read/1P3-146682121/internet-banking-in-the-u-s-japan-and-europe>

<sup>180</sup>Centeno Clara “*Adoption of Internet Services in the Enlarged European Union: Lessons from Internet Banking case*” June 2003, European Commission Joint Research Centre.

<sup>181</sup> Bank of Valletta Annual Report and Financial Statements 2017

powerful mechanisms to detect and prevent fraud within the internet payments domain.

In response to the rising level of cyber fraud the European Central Bank (ECB) published detailed recommendations for the security of internet payment and understanding of inherent risks among European Union Member States and established a foundation for consistent regulatory oversight of payment services, systems, and schemes.

### **2.3.1. European Banking Authority (EBA):**

The European Banking Authority was established with a motive to maintain an integrated approach for the supervision of banks across the European Union. It is a specialized agency to maintain the bank and financial organization across the states of Euro European Union (EU). Applicability of a single set of rules within European Union states to every banking or financial institution was the most important task for European Banking Authority. It is the duty of European Banking Authority to ensure the applicability of common rules to all banking institutions and make customers or their citizens aware about the law in a consistent and harmonized way.<sup>182</sup> EBA also provides the regulatory framework within the European Union in order to maintain the integrity and efficiency of banking among the States. It also contributes to maintaining financial stability across the Union. In addition, the EBA has an important role other than maintaining financial stability in the EU

---

<sup>182</sup>The European Banking Authority at a Glance URL: <https://eba.europa.eu/sites/default/documents/files/documents/10180/1401372/e8686db2-6390-4c52-ad06-bc8d24b7aeb5/EBA%20AT%20A%20GLANCE.pdf> (visited on 13.6.2020)

by promoting consumer protection and their interest with regards to maintaining harmony among the European Union.<sup>183</sup>

### **2.3.2. European Central Bank:**

“European Central Bank (ECB) is considered to be the central bank to govern all the banks of European Union. European Central Bank is responsible to maintain the monetary system within the States of European Union. It ensures the protection of consumer interest by providing stability in price and securing them from cyber fraud. They issue direction to all banks within the Union.<sup>184</sup> The ECB has been responsible to the banks after European Union decided to adopt a single currency.<sup>185</sup>

European Central Bank is an independent monetary union who work on their own and EU members adopting a single currency. They act without seeking any orders. The ECB is working as an independent institution. The institution doesn't work on the instructions from governments or any other EU countries, thus decide according to its discretion.<sup>186</sup> The differences in rules and controls among different countries were the factors leading to the crisis but now European Union adoption of single supervisory under European Central Bank will regulate the entire banking system of European Union member states.<sup>187</sup>

---

<sup>183</sup> *Supra* note 182

<sup>184</sup> <https://www.investopedia.com/terms/e/europeancentralbank.asp>

<sup>185</sup> <https://www.investopedia.com/terms/e/europeancentralbank.asp>

<sup>186</sup> [https://europa.rs/images/publikacije/HTEUW\\_How\\_the\\_EU\\_Works.pdf](https://europa.rs/images/publikacije/HTEUW_How_the_EU_Works.pdf)

<sup>187</sup> The European Union explained: How the EU works, November 2014 URL: [https://europa.rs/images/publikacije/HTEUW\\_How\\_the\\_EU\\_Works.pdf](https://europa.rs/images/publikacije/HTEUW_How_the_EU_Works.pdf) (visited on 13.3.2019)

### **2.3.3. Single Rule Book**

“The Single Rule Book is a set of rules which maintain stability in the banking transaction system throughout the European Union by setting a single rule book. European Union provides unified regulation among financial organizations. This rulebook was framed in 2009. The Single Rule Book focuses on the loophole that the banking sector which are making them weak to overcome their banking insecurities. The Single Rule Book ensured safety to all member states with a transparent set of rules in order to make it efficient banking regulations. The Single Rule Book makes it clear that the member states will be governed by a uniform rule book.<sup>188</sup> There is no such urgency to apply different rules for the banking system. It ensures financial institutions in a more transparent manner across the EU. The great thing about European nation is uniformity in banking laws; however, since previously European banking legislation was based on Directives, thus they were significantly divergent. Today a Single Rulebook addresses the shortcoming and aims to a more strong, transparent, and efficient.

### **2.3.4. Council of Europe’s Convention on cybercrime:**

The Convention on Cybercrime covers all the cyber crimes where a computer has been used as a target for accomplishing the crime. It is the one and only convention on a global level. It covers all the computer originated crime.<sup>189</sup> Its main objective of European Union is to enact uniform regulation through which we can combat the challenges of cybercrime.<sup>190</sup> Information technology

---

<sup>188</sup><https://eba.europa.eu/regulation-and-policy/single-rulebook>

<sup>189</sup> <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

<sup>190</sup> [http://repository.out.ac.tz/987/1/Anipha\\_Mwingira.pdf](http://repository.out.ac.tz/987/1/Anipha_Mwingira.pdf)

has brought a revolution in almost every aspect and it has changed society fundamentally. It has made their impact and many tasks are made easier to perform, most of the impact has been seen in technology communication. The development has been made socially and economically but along with development, there has been a dark side where crime is increasing along with their methods of committing crime or fraud in a more advanced way. Since such crimes are not able to restrict within any geographical boundaries or national boundaries. This new technology challenges the existing legal framework and nation laws are inadequate since they are only specified within limited boundaries or territory. The solution for such crimes needs to be addressed in an international scenario so the convention of Europe convention on cybercrime is one of them where it aims to meet the challenges in a new technology society.<sup>191</sup>

The Convention on Cybercrime is also known as the Budapest Convention on Cybercrime or the Budapest Convention. The Convention on Cybercrime entered into the force on July 1, 2004.<sup>192</sup> As of March 2016, 48 states have rectified the convention and additional six states have signed but not rectified it.<sup>193</sup> Till then it remains the most relevant international agreement on cybercrime and electronic evidence. “Convention also contains powers and procedures for the search of computer networks and interception.”<sup>194</sup>

---

<sup>191</sup>Salaheddine J. Juneidi, “Council of Europe Convention on Cyber Crime”, 2002 URL: [https://www.researchgate.net/publication/261363049\\_Council\\_of\\_Europe\\_Convention\\_on\\_Cyber\\_Crime](https://www.researchgate.net/publication/261363049_Council_of_Europe_Convention_on_Cyber_Crime)

<sup>192</sup>On 18<sup>th</sup> March 2004, Lithuania ratified the International Convention on Cybercrime enabling the instrument to enter into force on 1<sup>st</sup> July 2004.

<sup>193</sup>List of signatures and ratification of the Convention URL: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures> also see [http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018\\_.pdf](http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018_.pdf)

<sup>194</sup>ibid

The Budapest Convention is a criminal justice treaty that provides the criminalization of attacks by the means of computers and it is a law that guides the country's investigation authorities for making investigations for collecting electronic evidence.<sup>195</sup> The Convention has been drafted with the view to achieving a greater unity between its members with a uniform criminal regulation in order to protect the society from cybercrime<sup>196</sup> or computer networks.<sup>197</sup> It provides a framework for international cooperation between state parties to the treaty and it is the only multilateral agreement with an objective of harmonizing legislation on national cybercrime laws.<sup>198</sup> It is generally accepted that harmonization between the countries is essential if effective regulation of cybercrime is to be achieved.

The Budapest Convention has explained four different categories of offence (1) those offences which are against the maintaining confidential, ethics and information that are available in computers,<sup>199</sup> (2) offences that are related to computer<sup>200</sup> (related to computer fraud and forgery),<sup>201</sup> (3) offences related to child pornography and (4) criminal copyright infringement.<sup>202</sup> The Convention includes several principles and procedures to facilitate international cooperation for further investigations or proceedings and collection of

---

<sup>195</sup><https://www.ir.kiu.ac.ug/bitstream/20.500.12306/8947/1/img-0134.pdf> (visited on 16.5.2018)

<sup>196</sup>

[http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf) (visited on 24.8.2018)

<sup>197</sup> Preamble of Budapest Convention

<sup>198</sup>“Touring the world of Cybersecurity Law”, San Francisco Conference 2016 URL: [https://www.rsaconference.com/writable/presentations/file\\_upload/law-w04-global\\_cybersecurity\\_laws\\_regulations\\_and\\_liability.pdf](https://www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf) visited on 10/2/2019

<sup>199</sup> Chapter II Title 1 of Budapest Convention 2001

<sup>200</sup> <http://legalserviceindia.com/legal/article-3210-cyber-crime-a-hindrance-in-digitalworld.html>

<sup>201</sup> Chapter II Title 2 of Budapest Convention 2001

<sup>202</sup> Clough Jonathan, “A World of Difference: The Budapest Convention on Cybercrime And The Challenges of Harmonisation”, URL: [https://web.archive.org/web/20160430024621/https://www.monash.edu/\\_\\_data/assets/pdf\\_file/0019/232525/clough.pdf](https://web.archive.org/web/20160430024621/https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf) visited on 2/9/2018

electronic evidence.<sup>203</sup> As per Budapest Convention “Computer system is a device which is interconnected and it performs processing of the system automatically.”<sup>204</sup>

According to this Convention every nation must adopt the international convention as well as domestic law for cybercrime in order to deal with cyber criminals”<sup>205</sup> when they knowingly and without prior permission the owner tampered with the computer system.<sup>206</sup> Article 5 states that there must be a legislative measure that intentionally does the serious hindering with the functioning of a computer system.<sup>207</sup> Misuse of devices such as a “computer password, access code or similar data that can hamper the system and may even get corrupted”<sup>208</sup> as it is also considered as a criminal offence.<sup>209</sup>

Even though there is no single statute legislation or framework with related to cyber fraud, Budapest Convention has dealt with the offences with related to computer fraud where it states that, “state must have their own legislative measure so that they can frame regulation for cyber offences under their own

---

<sup>203</sup>Convention on Cybercrime Council of European Treaty URL: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

<sup>204</sup>Article 1(a) of Convention on Cybercrime 2001 URL: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>

<sup>205</sup> <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>

<sup>206</sup>Article 2 of Convention on Cybercrime: Illegal access- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

<sup>207</sup>Article 5 of Convention on Cybercrime: System Interference- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

<sup>208</sup> [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

<sup>209</sup>Article 6 of Convention on Cybercrime

domestic law, when accused knowing tries to alter delete or change the data stored in computer or temper computer system”<sup>210</sup> with a fraudulent or dishonest intention for personal benefits.<sup>211</sup>

The Convention sets out the investigative power in Chapter 2 Section 2 with regards to the digital investigation. “It ensures expeditious preservation of traffic data and disclosure to the competent authority to identify the service provider through which the data has been transferred.”<sup>212</sup> Article 19 empowers its “competent authority to adopt legislative measures to make search or access of computer systems where data has been stored. The competent authority must be empowered to collect the computer system that has been found during investigation or even can make different copies of seized documents.”<sup>213</sup>

---

<sup>210</sup> *Supra* note 209

<sup>211</sup> Article 8 of Convention on Cybercrime

<sup>212</sup> Article 17 of Convention on Cybercrime - Expedited preservation and partial disclosure of traffic data URL: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

<sup>213</sup> Article 19 of Budapest Convention: Search and seizure of stored computer data- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



Chapter III of the Convention “set out the guidance for establishing coordination for international issues.”<sup>214</sup> Article 23 suggests parties must have coordination among each other with the mutual agreement treaty for the purpose of investigation.<sup>215</sup> Article 25 to 34 set out procedures for mutual assistance in accordance with the request from one party to another party to assist in making an investigation.

For the collection of electronic evidence countries must have coordination through multilateral treaties or mutual Assistance Treaty.”<sup>216</sup> According to Article 25 of Budapest Convention, in case of urgent circumstances, each party can “make requests for coordination through fax or email”<sup>217</sup> or including the use of encryption where necessary. “The nation must act within

---

<sup>214</sup>Chapter III Section 1, Title 1- General Principle for International Co-operation URL: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

<sup>215</sup>Article 23 of Budapest Convention: The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigation or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

<sup>216</sup>Article 25 of Convention on Cybercrime: General principles relating to mutual assistance

<sup>217</sup>Article 25 of Budapest Convention: General principles relating to mutual assistance- 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

their jurisdiction of their domestic law and without prior request send collected information to another party if they consider it will assist in their investigation or proceedings.”<sup>218</sup> In a case where there is no mutual assistance treaty or agreement, the authority must appoint an officer who can be responsible enough to send and respond to their assistance.”<sup>219</sup> In the case of

---

<sup>218</sup>Article 26 of Budapest Convention: Spontaneous information-

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for cooperation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

<sup>219</sup>Article 27 Budapest Convention: Procedures pertaining to mutual assistance requests in the absence of applicable international agreements- 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, order public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party

emergency, the country needing for assistance can make the request directly from the court.<sup>220</sup> The Procedure for investigation any country can make a request for assistance for collecting data stored in the system.<sup>221</sup>

#### **2.4. Comparison of Indian banking system with European Union.**

Reserve Bank of India (RBI) is the sole central bank for the entire banks situated in India. It provided different guidelines, policies with regards to the functioning of banking transactions. With the adoption of information communication technology there brought a swift change in the banking sector and banks started providing internet banking services to their customers. There brought a shift from traditional banking systems to internet banking systems where they were providing better customer facilities along with their convenience. In European Union there are altogether 28 member States for which they have established a single set of rules which can be applicable to all banking institutions. They have provided common rules which are “applied for banking supervisors across the European Union in a consistent and harmonized way.”<sup>222</sup>

---

through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority

<sup>220</sup> Article 27.9.a of Convention on Cyber crime- In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

<sup>221</sup> Article 33 & 34 of Convention on Cybercrime

<sup>222</sup> <https://eba.europa.eu/sites/default/documents/files/documents/10180/1401372/e8686db2-6390-4c52-ad06-bc8d24b7aeb5/EBA%20AT%20A%20GLANCE.pdf>

After the adoption of internet banking there comes a different cyber challenges such as cyber fraud, illegal transaction of money via skimming, debit or credit card fraud, ATM fraud, phishing, vishing and many more. So in India RBI from time to time provides with the guidelines for controlling the cyber fraud issues but in the name of cyber law there is only one act i.e. Information Technology Act 2000 (Amendment Act 2008) which is actually inadequate to deal with cyber fraud issues. Indian judiciary has to deal with the cases of cyber fraud with help of other penal laws and other laws such as Indian Penal Code, Indian Contract Act, Indian Evidence Act, Criminal Procedural code and Information Technology Act 2000. Even European Banks have adopted different strategies when incorporating Internet technologies into their services such as creation of internet only bank, the addition of internet as a complementary distribution channel, a thorough restructuring of bank services production processes making use of new information and telecommunication technologies (including, but not limited to, Internet technology), creation of an Internet bank as a subsidiary of the bricks and mortar bank, with a new brand, targeting complementary consumer segments, or creating an Internet bank as a financial supermarket or aggregator, moving away from the traditional vertically integrated model of financial product creation and distribution.<sup>223</sup> But their own separate convention that deals with cyber crime and the Convention on Cybercrime are known as Budapest Convention on cyber crime or Budapest Convention which cover entire European member states. The Budapest Convention provides guidelines to all the members of European Union to combat the challenges of cyber frauds.

---

<sup>223</sup>Centeno Clara “*Adoption of Internet Services in the Enlarged European Union: Lessons from Internet Banking case*” June 2003, European Commission Joint Research Centre.

Due to lack of international coordination on cyber issues as a result there is no centralized international cyber threat information sharing or a common computer incident response team. There are conflicts among the sets of laws among the different countries therefore there is no single international framework for cyber issues. Worldwide, governments are struggling not only with the increasing levels of cyber frauds but also with the complexities of securing electronic evidence. It is only with a minuscule portion of evidence it will bring justice. It is the failure of the government to protect the rights and privacy of individuals otherwise they will lose faith in the rule of law. Council of Europe's Cyber crime is currently addressing the challenges for securing e-evidence where the data is distributed over different service providers, locations and the jurisdictions where mutual legal assistance is often not feasible.<sup>224</sup> While India is also confronted with the same challenges and the more real world crime involves cyber related issues than there is greater need for law enforcement officers, prosecutors or judges to have the skills of electronic evidence. Cyber fraud requires electronic evidence which is transnational in nature and it even includes foreign jurisdiction where there is a need for international cooperation. Most Mutual Legal Assistance (MLA) is required for collecting electronic evidence of cyber fraud and financial crimes. Mutual Legal Assistance is all about cooperation between competent authorities. India so far has not signed the Budapest Convention. Jurisdictional issues have posed a great challenge in front of Indian cyber security establishment when trying to tackle any form of cyber fraud in the digital age. The Budapest Convention aims to establish an alternative framework to resolve all the

---

<sup>224</sup> India and the Budapest Convention: Why not? URL: [India and the Budapest Convention: Why not? | ORF \(orfonline.org\)](http://indiaonline.org)

issues related to cyber by establishing 24 x 7 points of contact network.<sup>225</sup> India to overcome the challenges they must be the signatory member of Budapest convention.

In India there is no uniform Cyber law which can deal with challenges of Cyber fraud. It is always in need to check the parameter to what extent the crime constitutes cyber fraud. There are no cases which have set any landmark judgment for the punishment in crime of Cyber fraud. Cases of Cyber fraud are raising everyday but only few are registering and there has been a big question of safety of customers.

---

<sup>225</sup> India and the Budapest Convention: To sign or not? Considerations for Indian stakeholders – The Internet Democracy Project

## CHAPTER THREE

### ISSUES OF CYBER FRAUD

#### 3.1. Introduction:

With the emergence of the internet, the world has become a global village. It has created a virtual world with no boundaries, which provide people with ample opportunities. Cyberspace has been a boon to human civilization, where the internet keeps connected to people around the globe. It offers opportunities to develop their business and makes it possible to reach an international market beyond boundaries.<sup>226</sup> In the 21st century the development of Information Technology affects every individual all over the world. With the growth of technology it leads to the new types of digital crime in cyberspace. The usage of computers becomes more popular with the expansion of technology. Information Technology (IT) has provided equal opportunities to access any information, data storage, analyze etc.<sup>227</sup> For the past two decades, technology has become an integral part in the individual lives, it has changed the way the people work, study, and communicate. Just in a few seconds anyone can share their photos, videos, and email with their friends or dear ones. But the technology has become a new medium for conducting misconduct, to threaten, harass or even cause harm to others.<sup>228</sup> With time technology is improving, which influences the way people interact and communicate with others.

---

<sup>226</sup>Talib Mohammad & Sekgwathe Virginia, "E-Crime: An Analytical Study And Possible Ways to Combat," Volume 2 May 2012, published by International Journal of Applied Information Systems URL: <https://research.ijais.org/volume2/number2/ijais12-450261.pdf>

<sup>227</sup> Dr. Farooq Ahmad, "Cyber Law in India Law on Internet", 4<sup>th</sup> Edition (2015) New Era Law Publications

<sup>228</sup> Steven D. Hazelwood & Sarah Koon-Magnin, "Cyber Stalking and Cyber Harassment Legislation in the United State: A Qualitative Analysis," Vol 7 Issue 2 July 2013, International Journal of Cyber

Nowadays, Cyber fraud often makes headline news, but the number of fraud detected and prosecuted is just the tip of the iceberg. “The significantly offence of cyber fraud is not included in Information Technology Act, 2000 and it has not provided clarity.”<sup>229</sup> All the major financial institutions worldwide use computers to carry out their business, and vast sums of money are transferred through computers, i.e., via, electronic medium. Internet fraud constitutes about one- third of all cyber crimes and it has increased very fast by a substantial percentage over the past years. As we can see, these businesses on the internet are the most profitable and easy earning money.

In the banking sector, cyber fraud is conducted using online technologies to transfer money to different accounts. Banking frauds are categorized under cyber deception, which includes immoral activities of stealing credit card fraud and other online modes of committing fraud.<sup>230</sup> As computer crimes have been rampantly increasing, it's becoming more challenging to cyber police worldwide. We can see that there are differences between traditional crime and modern crime or cyber fraud as it comes under the category of cyber crime. “In modern crime, there is diversification of criminal phenomena, modernization or advancement of criminal methods resulting in serious consequences and found more difficulty in investigation and collection of evidence.”<sup>231</sup> Cyber fraud is different from traditional crime cases in finding clues, filing for investigation, identifying sites, collecting and protecting evidence, judicial identification, and legal proceedings.

---

Criminology.

URL:

<https://www.cybercrimejournal.com/hazelwoodkoonmagninijcc2013vol7issue2.pdf>

<sup>229</sup>Bangali Dr. Swapnil Sudhir & Bangali Dr. Harita Swapnil, In -Built Challenges for Information Technology Law in India, International Journal of Advanced Research (2016), Volume 4, Issue 6, URL: [http://www.journalijar.com/uploads/973\\_IJAR-10800.pdf](http://www.journalijar.com/uploads/973_IJAR-10800.pdf) (visited on 5.6.2020)

<sup>230</sup>Raghavan A.R and Parthiban Latha, " The Effect of Cybercrime on a Bank's Finances," Vol.2 Feb 2014, International Journal of Current Research and Academic Review URL: <http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf>

<sup>231</sup> Wu Yanbo, Xiang Dawei, Gao Jing Ming & Wu Yun, “Research on Investigation and Evidence collection of Cybercrime Cases”, 2018 IOP Con. Series: Journal of Physic: Conf. Series 117 (2019)



“What is the Internet? The Internet is a collection of interconnected networks of computers. The Internet is interconnected networks. The Internet carries numerous information. The Internet has created a platform for new creation. It has a capacity to create more interaction and communication of different information. The Internet is like a net where hundreds of thousands of different computer networks use common data transfer protocols to exchange information with other computers. It is like a chain in which one computer is connected with another. It has a quality of rapidly transmitting the information with the facility of automatic transmission where transmission is not possible due to damage or non-availability of link. The Internet uses the language of common communication protocol called Internet Protocol (IP).<sup>232</sup> “Internet working includes a technical design and a management structure. The technical design is founded on a complex, interlocking set of hierarchical tree-like structure like Internet Protocol addresses and domain name,<sup>233</sup> mixed with networked structure like packet switching and routing protocol all tied together with millions of sophisticated software that continues to get better all the time.”<sup>234</sup> “There are various standard devices, technology and protocol which work together to make the internet function properly this includes routers, TCP<sup>235</sup> /IP<sup>236</sup> protocol, HTML<sup>237</sup> etc.”<sup>238</sup>

---

<sup>232</sup>Internet Protocol (IP) is language used for communicating data across a packet-switched internetwork. The Internet Protocol (IP) is a protocol or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. An IP address is a unique identifier assigned to a device or domain that connects to the internet. See: <https://www.cloudflare.com/learning/network-layer/internet-protocol/>

<sup>233</sup>Domain Name means location of an entity on the internet. Domain names are the human-friendly forms of an Internet Protocol address, and are commonly used to find the websites. It can be seen as an online identity of a particular person, organization, establishment etc. for example if we search Facebook on google then at the top of the browser window in the URL bar there it starts with “http://” in the address bar. The second part of the URL is the domain. Domain name consists of two parts i.e. facebook.com, where “.com” is the top level domain.

<sup>234</sup> Dr. R.K. Chaubey, “*An Introduction to Cyber Crime and Cyber Law*,” Published by Kamala Law house Kolkata, 2008 edition(2009 reprinted)

<sup>235</sup> Transmission Control Protocol (TCP)

<sup>236</sup> Internet Protocol (IP)

To address cyber fraud, the nature of the problem needs to be understood in detail. In this chapter, all the issues like the definition of cyber fraud, essentials of cyber fraud, investigation mechanism issues, prosecuting issues, issues of consumer liability, transnational issues, and jurisdictional issues are discussed.

### **3.2. Fraud and Cyber Fraud: definitional issues**

There is no such definition for cyber fraud defined under any of the statute. Absence of definition proves to be problematic for law enforcement. This creates challenges for dealing with cases of cyber fraud.<sup>239</sup> So to understand cyber fraud and the parameter up to which it can constitute cyber fraud, firstly, we need to define and understand cybercrime. There is no agreed definition of 'cybercrime' so to understand what is meant by cyber crime it is helpful if we start with the definition of 'cyberspace.' "The term 'cyberspace'" was first used by William Gibson where he describes it as a code or cryptograph which transforms it into a meaningful text message. It is used and associated with computers, information technology, the internet along with other diverse internet cultures."<sup>240</sup> "Whatever communication and actions occur with Information Technology in the virtual world are taking place in cyberspace. The Internet has connected every network and Cyberspace a electronic global village where it can communicate without any boundaries."<sup>241</sup>

---

<sup>237</sup>Hypertext Markup Language (HTML) is the language used to describe web pages and is still used as the main interface language to the web. It is the road signs of a web page. See: <https://www.investopedia.com/terms/h/html.asp>

<sup>238</sup>Douglas E-Commerce, *The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works* 4th Edition 2006.

<sup>239</sup> [https://www.researchgate.net/publication/280488873\\_Cyber\\_crime\\_Classification\\_and\\_Characteristics](https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics)

<sup>240</sup>Arya Nidhi, *Cyber Crime Scenario in India and Judicial Response* URL: [https://www.researchgate.net/publication/334124155\\_Cyber\\_Crime\\_Scenario\\_in\\_India\\_and\\_Judicial\\_Response](https://www.researchgate.net/publication/334124155_Cyber_Crime_Scenario_in_India_and_Judicial_Response)

<sup>241</sup>Anirudh Rastogi, "Cyber Law of Information Technology," 1<sup>st</sup> Edition 2014 Published by LexisNexis

Cyberspace is a virtual computer world where communication or interaction takes place in the electronic<sup>242</sup> information, conduct business, play games and engage in political discussions etc.<sup>243</sup> This indicates that cybercrime takes place with the help of networked computers, or internet technology<sup>244</sup> or a crime is facilitated by computer or internet.<sup>245</sup> Cybercrime as defined by “National Cyber Crime Reporting Portal”<sup>246</sup> means “any unlawful act where computer device or communication device or computer networks are used in order to commit or facilitate the act of commission of crime.”<sup>247</sup>

Professor H.L.A Hart’s “Concept of Law said human beings are vulnerable by their nature so rule of law is required to protect them.”<sup>248</sup> “The Rule of law even applies to the virtual world and because of the vulnerable nature of computers it requires protection from cyber fraud.<sup>249</sup> There are certain vulnerabilities of computers as they have a unique character where it can store data even in small storage or there are possibilities of easy unauthorized access due to technology complexity. Operating system of computers is composed of millions of codes where every individual mind

---

<sup>242</sup> [http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018\\_.pdf](http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018_.pdf)

<sup>243</sup> Meaning, Concept and Classification of Cyber crimes URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11\\_cha%5bpter%203.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11_cha%5bpter%203.pdf) (visited on 1/2/2020)

<sup>244</sup> Association of Chief Police Officer (ACPO) of England define cybercrime <https://research.ijais.org/volume2/number2/ijais12-450261.pdf>

<sup>245</sup> Talib Mohammad & Virginia Sekgwathe, E-Crime: an analytical study and possible Ways to Combat, International Journal of Applied Information System Volume 2, May 2012 URL: [ijais12-450261.pdf](https://ijais12-450261.pdf)

<sup>246</sup> National Cyber Crime Reporting Portal is an initiative of Government of India to facilitate victims or complainants to report cybercrime complaints online. This portal caters all types of cyber crime complaints including online Child Pornography, Child Sexual Abuse Material, online and social media crimes, online financial frauds, ransomware, hacking, cryptocurrency crimes and online cyber trafficking. Even we can make anonymous complaint reporting for Child Pornography or sexually explicit content such as Rape or Gang Rape. See: <https://taxguru.in/corporate-law/national-cyber-crime-reporting-portal.html>

<sup>247</sup> URL: Cybersecurity in India - Lexology

<sup>248</sup> Pati Prathasarathi, Cyber Crime URL: CYBER CRIME (naavi.org)

<sup>249</sup> <https://www.slideshare.net/RanjanaAdhikari/cyber-crime-9203478>

cannot understand so cyber criminals take advantage of these lacunas and penetrate with computer systems.<sup>250</sup>

Cyber fraud is a white collar crime which comes under the category of cybercrime. India having many regulations covering all crimes got inadequate regarding cyber fraud. To be more specific, cyber fraud does not have any agreed definition until today's date, so to define cyber fraud; we have to understand what fraud is and what constitutes fraud. Penal legislation of India i.e. Indian Penal Code 1860 has also failed to define fraud. The Code explains the terms fraudulently,<sup>251</sup> dishonestly,<sup>252</sup> and covers offences like cheating,<sup>253</sup> forgery,<sup>254</sup> etc. Fraud<sup>255</sup> has been extensively defined under civil law remedies, i.e., the Indian Contract Act, 1872. RBI being a central bank has also not defined "fraud," but RBI has suggested definition of fraud in the context of electronic banking.<sup>256</sup>

"The fraud is a wide term that includes any behavior where one person tried to have dishonest or unlawful advantage over another person.<sup>257</sup> Fraud in simple terms means to cheat another person in order to gain something over the victim, causing him a loss. Through this, we can understand cyber fraud in deliberate deception of something in order to gain financial need through the medium of modern technology i.e., computers, keyboards, and the internet. Lack of a specific definition of cyber fraud is

---

<sup>250</sup> Cyber Space Jurisprudance URL: <http://assets.v mou.ac.in/PGDCL01.pdf>

<sup>251</sup>Section 26 of Indian Penal Code, 1860

<sup>252</sup> Section 24 of Indian Penal Code, 1860

<sup>253</sup>Section 415 of Indian Penal Code, 1860

<sup>254</sup>Section 463 of Indian Penal Code, 1860

<sup>255</sup>The Indian Contract Act, 1872, Section 17.

<sup>256</sup>The Report of RBI Working Group on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds which read as under:-

"A deliberate act of commission by any person carried out in the course of a banking transaction or the book of accounts maintained manually or under computer systems in the bank, resulting into wrongful gain to person for a temporary period or otherwise, with or without any monetary loss to the bank". See: <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf>

<sup>257</sup>URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/129054/10/06\\_chapter%201.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/129054/10/06_chapter%201.pdf) (visited on 21/2/2020)

creating hurdles in further investigation and prosecution. It's been a decade for us dealing with the issues of cyber crime, so India implemented the Information Technology Act, 2000, and further made amendments of IT Act, 2008, but it does not include cyber fraud. As per the close observation of RBI, the bank fraud cases were technology-related frauds conducted through internet banking, ATMs, credit/debit cards. It's been essential to consider this cyber fraud as a severe crime. At the time, lawmakers must not feel necessary or just overlooked the issues of cyber fraud, creating chaos in a banking institution or general public in the present scenario.

### **3.2.1. Essentials of Cyber Fraud:**

The term cyber fraud does not have any specific definition provided by any statute or legislature. It cannot be defined due to its sophisticated nature since it involves fraud relating to computer and computer techniques. Cyber fraud falls under the different types of cybercrime, and the development of technology has brought a new way of committing a crime, which is different from other conventional crimes. “The feature of cyber fraud is that they are easy to commit, difficult to detect because it is a borderless crime, and even harder to prove.”<sup>258</sup> Cyber fraud is committed whenever there is an opportunity and now it has become one of the easiest mediums to earn money. Every crime must be considered in two parts: the physical act of the crime (*actus reus*) and the mental intent to do the crime (*mens rea*). In cyber fraud also these both elements of crime can be found.

---

<sup>258</sup>The Law Relating To Cyber Crime In India URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08\\_chapter%203.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08_chapter%203.pdf) (visited on 27/3/2020)

### 3.2.2. Types of Cyber fraud:

There are certain offences which can be categorized as cyber fraud; they are as follows:

#### i. **ATM fraud:**

It's a fraudulent activity in which a criminal uses the ATM card or the cloned ATM card of another person so that they can withdraw money from the card holder's account. It is done by obtaining a PIN number from the ATM device.<sup>259</sup> There are various kind of ATM fraud such as Card Shimming,<sup>260</sup> Card Skimming,<sup>261</sup> Card Trapping,<sup>262</sup> Jamming of Keyboard.<sup>263</sup> Most of the ATM fraud occurs due to the negligence of customers by giving up their Personal Identification Number (PIN) to their relatives or divers to withdraw their money from the ATM from them. Most of the time ATM fraud occurs because of carelessness of customers themselves by giving their money to their diver or relatives to withdraw the money from the ATM for them. Fraudsters place certain devices above the ATM card reader slot to obtain the card details.<sup>264</sup>

---

<sup>259</sup><https://www.bajajfinserv.in/what-is-atm-fraud-and-types-of-atm-fraud> visited on 20/1/2020

<sup>260</sup> Card Shimming is done by installing a shimming device on an ATM machine for getting data from the card's chip. It captures magnetic strip equivalent data.

<sup>261</sup> Card Skimming includes stealing the electronic data of a card in order to imitate the card completely.

<sup>262</sup> Card Trapping includes stealing the ATM card by installing a device at the ATM.

<sup>263</sup> Jamming of Keyboard: The fraudster will jam important buttons on the ATM machine keyboard as Cancel and Enter buttons so that the transaction is unsuccessful

<sup>264</sup>Jain Shubhra Jain, ATM Frauds- Detection & Prevention, International Journal of Advances in Electronics and Computer Science, Vol. 4, Issue- 10, October 2017 URL: [http://www.iraj.in/journal/journal\\_file/journal\\_pdf/12-410-151445396982-89.pdf](http://www.iraj.in/journal/journal_file/journal_pdf/12-410-151445396982-89.pdf) (visited on 23/7/2019)

In “**Senior Branch Manager v. Binoy Kumar Roy, Order dated 03.01.2017**, the case was related to unauthorized withdrawal of money from the ATM of Appellant. As per complaint Rs. 15, 000/- was withdrawn without his notice. The Court held that ATM fraud is not a new type of fraud in India and slowly with time it is weakening the financial institution of our country.”<sup>265</sup> “ATM scams are gradually increasing over the years. The real reasons for failure of ATM networks include interceptions, insider involvement or sometimes both. Reserve Bank has been receiving complaints that they are receiving counterfeiting banknotes through the ATM. ATMs fraud is worse than credit card frauds.”<sup>266</sup>

“Fraudster in July 2018 hacked the bank system of Canara Bank ATM and made fraudulent transactions from different bank accounts in Kolkata an amount of 20 lakh rupees. After making an investigation, the investigating officer came to know that the accused had collected more than 3000 ATM user account details. The accused collected ATM card details through skimming devices and they made transactions of minimum Rs. 10, 000/- and maximum amount up to Rs. 40, 000/- from their account.”<sup>267</sup> On 5<sup>th</sup> August 2018, Delhi police arrested two men who were working with an international gang to conduct cyber fraud using skimming devices to extract the bank account details. “Recently after receiving complaints of unauthorized

---

<sup>265</sup> Senior Branch Manager, United Bank of India v. Binoy Kumar Roy, Order dated 03-01-2017 URL: <https://www.casemine.com/judgement/in/5e1f03929fca19162beeba01>

<sup>266</sup>V. Gopal Krishna and G. Usha, ATM Banking: Legal Issue of Security Concern, ICFAI Journal of Banking Law, 2007

<sup>267</sup>Major Cyber Attacks on India (Exclusive New) dated 20th January 2020, URL: <https://www.testbytes.net/blog/cyber-attacks-on-india/> (visited on 2<sup>nd</sup> February 2020).

ATM transactions Goa Police nabbed three Bulgarians for involvement in ATM skimming at different places within the state based on local intelligence and analysis of nearby CCTV footage. They had recovered several laptops and skimming cameras from the accused.”<sup>268</sup>

“Kolkata police arrested four foreign nationals who allegedly hacked several ATMs of State Bank of India. They hacked their account details with the cloning devices in card slots in the ATM of State Bank of India.”<sup>269</sup> Also on 20 October 2020 a 39 year old woman, a cancer patient, is alleged to have lost Rs. 25,000 just in 3 minutes and cash was withdrawn from ATM in Tollygunge when the woman was at home. Bank did not help her rather asked her to fetch a police report for refund and it was only after involvement of the anti-bank fraud section and cyber cell got involved that they found the leads of cases.<sup>270</sup>

In 2019 two students were arrested by Mumbai police for ATM fraud of Rs. 1 crore. The accused were Asif Khan (19 years) of Rajasthan and Asmat Khan (21 year) of Haryana. They used more than 50 ATM cards for withdrawal of cash. Police said that the accused had learned to switch off the ATM machine just before the dispensed. They collect the money and later claim a refund from the bank for the deduction amount from their account. They could check the record and found the

---

<sup>268</sup>The Times of India dated: September 23, 2020

<sup>269</sup><https://www.ndtv.com/india-news/atm-fraud-in-assam-4-foreigners-hack-atms-dupe-sbi-customers-of-crores-arrested-near-kolkata-police-2135234> Dated: November 19, 2019

<sup>270</sup> The Times of India dated: November 21, 2020



transaction failed due to the machine going offline and refunding the amount.<sup>271</sup>

In Mumbai, a fraudster cheated on Mehta, a 78 year old man, via telephonic conversation with Vajay Chauhan who referred to himself as a bank official of a private bank. That person informs the elderly man about the expiration of his credit card and asks him for his credit card details, CVV number along with OTP generated on his mobile phone for the activation of credit card. After sometime he got a message stating 2.34 Lakh deducted from his account.<sup>272</sup> Country witness increased in ATM fraud cases RBI revealed that Maharashtra reported 233 cases in 2018-2019 where people lost 4.8 crore to bank fraud, highest in the entire country.<sup>273</sup> Reserve Bank warned those who are using online banking that fraudsters might wipe out all the customers' balance by using Unified Payment Interface (UPI).<sup>274</sup>

“In October 2020 two incidents of ATM Fraud came before Pune police where two similar incidents had occurred in ATM of Canara Bank. In the first incident three unidentified persons entered the ATM of Canara Bank in Dhankawadi, they allegedly inserted a credit card in the machine and opened the display then tempered it with the internet cable and reset the button. The accused withdrew Rs. 5.66 lakh which was not recorded in the electronic machine computer system. In the second incident, two unidentified persons withdrew Rs 2.46 lakh from

---

<sup>271</sup> The Indian Express dated: February 3, 2019

<sup>272</sup><https://indianexpress.com/article/cities/mumbai/mumbai-cyber-fraudsters-dupe-78-year-old-of-rs-2-32-lakh-6638707/>

<sup>273</sup> Business Standard dated: July 22, 2019

<sup>274</sup> Business Standard dated: February 18, 2019

Canara Bank ATM in Sadashiv Peth. In both cases police found that the transaction details were not recorded in the electronic system. FIR has been lodged in both the incidents for further investigation.”<sup>275</sup>

ii. **Carding:**

“Carding is illegal in India and it means using credit card or debit card details fraudulently for the purpose of buying goods and services.”<sup>276</sup> It is an unauthorized account transaction when fraudsters use duplicate ATM cards to withdraw money from victim’s accounts for their benefit. Fraudster can steal card detail in several different ways such as sending email asking you to enter card details on the fake website pages. Sometimes even you will get some random call in the name of a bank official collecting details for ATM card renewal or for the purpose of Know Your Customer (KYC) updates. The fraudster or hacker has been more advanced every time they create new methods to crack the security system.

There has been a recent credit card point fraud incident in Delhi where a 73 year old retired professor of Delhi University was cheated by offering him to redeem credit card points. During the investigation the victim told that he received a bulk of messages to redeem credit card points so in order to redeem those points he visited the website by link which was provided there in messages and he updated their card details. But after sometime he received a SMS alert of the Rs.60 000/-

---

<sup>275</sup> The Indian Express dated: October 17, 2020

<sup>276</sup>Peretti Kimberly, “Data Breaches: What the Underground World of Carding Reveals,” Santa Clara High Technology Law Journal, Volume 25, Issue 2, 2009. URL: <https://core.ac.uk/download/pdf/149256649.pdf> (visited on 7.3. 2020)

deduction from his account. “Police arrested a man named Jha (30 years) for cheating a retired professor in the context of redeeming or collecting credit card points. During interrogation, the accused disclosed that he had sent similar messages with the same link to many people in order to obtain credit card details.”<sup>277</sup>

Another credit card fraud has come to light where an agent of a bank was arrested by Delhi police for making unauthorized fraudulent transactions of Rs. 69, 000/- he has obtained details through mobile application installation.<sup>278</sup> Police recovered two mobile phones used for making transactions and credit/debit cards of two banks. Accused has done all the transactions through Paytm and Mobikwik.<sup>279</sup>

iii. **Cheating & fraud:**

Stealing password and account details with the wrongful intention which leads to the act or omission of fraud and cheating with the help of technology. “A Russian computer hacker, Boss Burkov of St. Petersburg, was sentenced to nine year jail in a U.S. prison after pleading guilty to running a site on the internet for stolen cards. Inside the website the member could buy and sell stolen credit card numbers. He ran the website Card Planet, where they offer stolen credit card numbers for sale from \$3 to \$60. The website even guaranteed money

---

<sup>277</sup>NDTV Press Trust of India dated: July 10, 2020 URL: <https://www.ndtv.com/delhi-news/retired-delhi-university-professor-loses-rs-60-000-in-credit-card-points-fraud-cops-2260816>

<sup>278</sup> <https://www.ndtv.com/delhi-news/retired-delhi-university-professor-loses-rs-60-000-in-credit-card-points-fraud-cops-2260816>

<sup>279</sup> India Today dated: September 10, 2020 URL: <https://www.indiatoday.in/crime/story/delhi-police-arrests-bank-agent-held-for-credit-card-fraud-1720662-2020-09-10>

back in case card numbers didn't work. Burkov was running a huge business of online selling stolen card numbers from any place.<sup>280</sup>

In 2020 Delhi police arrested five people including one woman for allegedly cheating more than one thousand credit card holders in the past two years for cyber fraud in central Delhi. The mastermind of the gang Pawan Singh B. Tech dropouts was the mastermind. The accused received card holder details from some bank staff and after that the accused called the account holder offering credit card upgrades. The fraudster keeps the victims busy talking to them and manipulating them into revealing their OTPs and withdrawing money from accounts within a second. The victim told police that he received a call from a woman offering herself as an executive officer of State Bank of India. In order to gain his trust the women gave account holder details such as birth date and bank details. After that she offered him credit card upgrade details and asked him to share OTP which will complete the upgrading process. Then after completing the conversation he received a SMS of a transaction of money to a different wallet account.<sup>281</sup>

Fraudsters steal from Shri Ram Janmabhoomi Teerth Kshetra Trust Rs. 6 lakh from their bank account. Fraudsters smartly used forged signatures in a cloned cheque to complete the transaction from the trust which was the fund of the Ram Temple in Ayodhya. The case has been

---

<sup>280</sup> AP News dated: June 26, 2020 URL: <https://apnews.com/article/83ee48ae2a98aeb9a03a45df9e83eac3>  
<https://www.ndtv.com/delhi-news/retired-delhi-university-professor-loses-rs-60-000-incredit-card-points-fraud-cops-2260816>

<sup>281</sup>The Times of India dated: September 4 URL: <https://timesofindia.indiatimes.com/city/delhi/delhi-gang-cheated-1000-credit-card-holders-in-2-years/articleshow/77923886.cms>

registered under Section 471,<sup>282</sup> 468,<sup>283</sup> 467,<sup>284</sup> 420,<sup>285</sup> 415<sup>286</sup> of Indian Penal Code 1860. Fraud only came to the notice when they received a call from the bank stating that a third forged cheque was placed for clearance. DSP said that this fraud has clearly shown negligence on the bank side because a serial number of the cheques has been compromised that allowed the fraudster to use a cloned cheque along with the forged signature. Police are still in search of a fraudster in this case.<sup>287</sup>

iv. **Phishing:**

“It is a process of tricking an organization or individual into imparting their confidential information with the purpose of misusing. The

---

<sup>282</sup> Section 471 of Indian Penal Code 1860: Using as genuine a forged document or electronic record- Whoever fraudulently or dishonestly uses as genuine any [document or electronic record] which he knows or has reason to believe to be a forged [document or electronic record], shall be punished in the same manner as if he had forged such [document or electronic record].

<sup>283</sup> Section 468 of Indian Penal Code 1860: Forgery for purpose of cheating- Whoever commits forgery, intending that the [document or electronic record forged] shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

<sup>284</sup>Section 467 of Indian Penal Code 1860: Forgery of valuable security, will, etc.- Whoever forges a document which purports to give authority to any person to make or transfer any valuable security, or to receive the principal, interest or dividends thereon, or to receive or deliver any money, movable property, or valuable security, or any document purporting to be an acquittance or receipt acknowledging the payment of money, or an acquittance or receipt for the delivery of any movable property or valuable security, shall be punished with [imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

<sup>285</sup> Section 420 Indian Penal Code 1860: Cheating and dishonestly inducing delivery of property- Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

<sup>286</sup> Section 415 of Indian Penal Code 1860: Cheating- 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 intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to “cheat”.

Explanation- A dishonest concealment of facts is a deception within the meaning of this section.

<sup>287</sup>India Today dated: September 10, 2020 URL: <https://www.indiatoday.in/india/story/fraudsters-steal-rs-6-lakh-from-ram-temple-trust-account-using-forged-cheques-1720533-2020-09-10>

process causes computer users to give their personal information. They usually attack or target those sites with a specific brand or entity from which they can get a huge sum of money.”<sup>288</sup> Phishing is a scam where a person willfully tries to collect consumer information such as card details, CVV number and OTP generated in the mobile phone of account holders.<sup>289</sup> The customer receives uninvited emails from financial institutions requesting the account holder to enter their internet banking username, password, or other personal details to access their account to receive their service benefit. Instructions are also provided for the customers which leads them to update their details but doing this they will automatically lose their money. Without being aware, fraudsters get access to the customer bank account and transfer the amount. There are growing numbers of reporting in phishing incidents, additional methods of protection are still required. More recent phishing attempts have started to target banks, customers of banks and online payment services. Additional efforts are needed for legislation, user training and technical measures.

Damages caused by the phishing ranges from the access of email to the substantial loss of money from the account through unauthorized transactions using different techniques of phishing. The perpetrators are opting this style of fraud because unexpected people are involved in this transaction and it can be done using account holder card details

---

<sup>288</sup>Meijerink Tristan Janothan, “ Carding Crime Prevention Analysis,” Politie Netherlands Police Agency, 2013 URL: [https://essay.utwente.nl/63027/1/Understanding\\_processes\\_of\\_carding\\_versie\\_7\\_31-1\\_word.pdf](https://essay.utwente.nl/63027/1/Understanding_processes_of_carding_versie_7_31-1_word.pdf) (visited on 20.1.2020)

<sup>289</sup>NASSCOM v. Ajay Sood and Ors 119 (2005) DLT 596, 2005 (30) PTC 437 Del URL: Success in any field of human activity leads to crime that need (delhicourts.nic.in)

and social security details. After obtaining all the details of the account holder they will create a fake account in the name of account holder, prevent customers from accessing their own account and misuse customers credit /debit card.

Phishing is considered to be the most common gateway to collect the information through sophisticated emails or by sending text messages on their mobile phone.<sup>290</sup> As per the information Reliance Jio Infocom has dragged Paytm over phishing attacks on its users and they are not trying to block those malicious text messages which are being sent to customers in the name of the bank or other service provider seeking their personal details. The liability of preventing financial fraud lies on banks and wallet companies such as Paytm as per the Reserve Bank of India mandate.<sup>291</sup> During the COVID-19 pandemic period there occurs large numbers of phishing cases. The Government of India had warned of phishing attacks and asked everyone to be alert regarding fake email ids. People were receiving messages or emails from fake websites claiming to be a part of financial aid enrolled by the government of India to deal with COVID-19. They were asking their for sensitive personal information as well as banking information where they can easily collect the account details and used for conducting frauds later on. Those email IDs were similar to the official government domains such as 'ncov2019@goc.in'. The government agency claims that user's shouldn't download or open such attachments from unsolicited emails

---

<sup>290</sup> The Economics Time Dated: August 23, 2019

<sup>291</sup> The Economics Time Dated: June 20, 2019

and if possible they should refrain completely from clicking on URL with such emails.<sup>292</sup>

In September 2020, Delhi police busted a nexus of cyber fraud that was operating phishing from Jamtara in Jharkhand. Jamtara in Jharkhand is considered as a hub for operating cyber crime in India. Incident occurred when victim call in toll-free number of Axis Bank which was provided in Google and call was not received as it was a fake number. But next time victim received a call from a bank employee and he sent the victim a link to resolve his issue. Soon after receiving the link, the victim clicked the link and lost Rs. 63,800/-. During investigation one number was traced and it was found to be registered in Jamtara Jharkhand, under the name of Nasim Ansari. On interrogation he disclosed all the details of the gang member and police found 15 different ATM cards, swipe machines and fingerprint scanner from the accused. In total police arrested six men and recovered 25 ATM cards, 1,78,5000, cheque books with three blank cheques.<sup>293</sup>

“We should not install any e-wallet or mobile banking app or any other payment system from the link sent by the message or email because it can lead to phishing. Government issued a warning for the user. Stop installing payment apps link sharing via email and SMS.”<sup>294</sup> For identifying phishing we must remember that a legitimate banking

---

<sup>292</sup><https://www.livemint.com/technology/tech-news/govt-warns-of-serious-phishing-attack-starting-today-bewa-re-of-this-email-id-11592718991047.html>

<sup>293</sup> India Today dated: September 10, 2020 URL: <https://www.indiatoday.in/crime/story/delhi-police-busts-cyber-fraud-nexus-having-roots-in-jamtara-jharkhand-1720307-2020-09-10>

<sup>294</sup>The Times of India Gadgets News dated: September 10, 2020 URL: <https://timesofindia.indiatimes.com/gadgets-news/do-not-install-paytm-or-other-mobile-payments-app-from-unknown-links-govt/articleshow/78037607.cms>



institution or financial institution will never ask for customers account details via email. If you need to initiate the transaction of details through emails over the internet to their website then you must look for indicators like sign or icon or URL to stand for secure transmission of information.<sup>295</sup>

v. **Skimming:**

It is a process of obtaining detailed information of credit cards and other additional card holder's detailed information to make payment on behalf of victims. "The skimmers attached within the card slot will copy magnetic strips from the bank cards by using the hardware modification. In which PINs are stolen by using a camera or by using a magnetic strip inside the card slot of an ATM. They even use fake keyboards on top of existing keyboard ATMs where they can collect the keys that were being used for transaction purposes."<sup>296</sup>

There is a case of E-wallet skimming which has become a trending cyber fraud. Mona Markar, a 45 year old woman ordered a saree via avkcart.com and payment was done on delivery but after a few days she found the saree was defective. So in order to get a refund she tried to contact customer care at info@avkcart.com but it did not work out. Mona google the number then contact customer care there she was told to download the Google Pay application in mobile to receive refund

---

<sup>295</sup>CA Mayur Hoshi, Phishing in India is becoming innovative, URL: <https://indiaforensic.com/understanding-phishing-india/> (visited on 20/1/2020)

<sup>296</sup> Meijerink Tristan Janothan, "Carding Crime Prevention Analysis," Politie Netherlands Police Agency, 2013 URL: [https://essay.utwente.nl/63027/1/Understanding\\_processes\\_of\\_carding\\_versie\\_7\\_31-1\\_word.pdf](https://essay.utwente.nl/63027/1/Understanding_processes_of_carding_versie_7_31-1_word.pdf) (visited on 20.1.2020)

but it turned out to be a loss of Rs. 1 lakh in place of refunding the amount Rs. 1 500 by simply clicking on the link. Cyber experts called these incidents as e-wallet skimming frauds.<sup>297</sup> In case of ATM skimming two Nigerian nationals were arrested for setting skimmer on the ATM machine in order to make unauthorized transactions. Skimmer is an illegal device which is fitted in ATM card slots through which they can obtain card details by copying it in the skimmer later on they cloned the card and carry fraudulent transactions. Police personnel seized a skimmer, memory card and cloned credit and debit card from the accused.<sup>298</sup>

In Skimming cases fraudsters always keep victims engaged in telephonic conversation and as per direction they start clicking the link and simply complete the process of transaction. Similarly, two Romanian couples were arrested in Delhi for ATM skimming fraud in Mumbai where people altogether lost Rs. 38 lakh. Fraudster couple came to India as tourists and they started installing skimmer in an ATM in Mulund. After copying the card details they made a cloned ATM and started withdrawing money from ATM in Delhi and Uttar Pradesh<sup>299</sup>

---

<sup>297</sup> Mumbai: Beware of E-wallet skimming, the trending cyber fraud URL: <https://www.dnaindia.com/mumbai/report-mumbai-beware-of-e-wallet-skimming-the-trending-cyber-fraud-2775826>

<sup>298</sup> The Indian Express dated: May 15, 2019

<sup>299</sup>DND India date: December 28, 2017 URL: <https://www.dnaindia.com/mumbai/report-2-romanians-held-in-delhi-for-atm-fraud-in-mumbai-2571039>

vi. **Vishing:**

A combination of 'voice' and 'phishing' is a phone scam designed to get the customer's personal information. It's similar to phishing, and instead of using emails, vishers use an internet telephone service (VoIP). "Fraudsters use emotional manipulation, and they oblige the victims into giving their personal details. The only goal of a visher is to steal your money, identity, or both."<sup>300</sup>

In 2018, a 59 year old retired official became victim by losing Rs. 1.10 lakh to a vishing fraud and the victim has bought a credit card with the limits of 5 lakh. While making the complaint the victim told police that he received a call from a person posed to be a government official and mentioned the victim's name and address to gain his confidence. After that the fraudster asked the victim whether he had brought any credit card and his making inquiry for verification purposes. With Conversation retired official gave his credit card details to the fraudster and even the OTP number. Within minutes he started receiving messages of transaction amounts of Rs. 20 000, Rs. 10 000 and Rs. 10 000 from his bank account. He didn't understand those messages and just ignored it. Next day also the victim received a call asking OTP for verification along with it got a message of transaction of Rs. 49 999, Rs 10 000 and Rs. 10 000. At that time he got suspicious by the call so he didn't give them OTP but there after he received a message stating that his credit card has been blocked and soon contact your bank

---

<sup>300</sup> "What is Vishing? Voice Phishing Scams Explained & How to Prevent Them", URL: <https://fraudwatchinternational.com/vishing/what-is-vishing/> (visited on 21.1.2020)

number. The victim, a retired official, then approached Gorega on police station and registered a case for cheating under Information Technology Act.<sup>301</sup>

In February 2020, three people were nabbed in the vishing fraud case and brought to Chennai. R. Dev Kumar (22years), Wilson Mathew (25 years), R. Deepak Kumar (21 Years) was arrested from Vasanth Vihar. Both of them migrated from Tamil Nadu several years ago and while working in call centers they learnt the trick of vishing. Police say that the modus operandi was calling victims for OTP (One-Time password) over phone calls and they claim themselves as bank officials and speak in local ;language Tamil. They cook many stories like their card has been blocked or they have won prizes or update their Aadhaar number.<sup>302</sup>

vii. **Financial Crimes:**

In this type of crime, the culprit tries to attack the users' networking sites by sending bogus mail or messages through the internet. They use credit cards by illegally obtaining passwords. “In Pune Rs. 94 crore online frauds was conducted in Cosmos bank in Pune by attacking the bank's system with malware. The fraudulent unauthorized transaction was made on 11th and 13th August 2018. The bank's first transaction lost Rs 80.50 crore with multiple ATM swipes in 28 different countries

---

<sup>301</sup>Express News Service dated: September 17, 2018 URL: <https://indianexpress.com/article/cities/mumbai/vishing-case-retired-best-official-loses-lakh-claims-police-5359514/>

<sup>302</sup>The Hindu dated: February 26, 2020 URL: <https://www.thehindu.com/news/cities/chennai/delhi-based-vishing-gang-held-for-cheating-hundreds-in-tamil-nadu/article30917302.ece>

and in the second attack, they lost 13.94 crore via Swift transfers.”<sup>303</sup>

“When money is withdrawn at ATMs, as soon as the card is swiped, a request will be sent to their respective banks and if the said account has sufficient balance then the bank automatically will allow the next transaction. In the case of Cosmos bank, a virus attack created a gateway system to bypass the core banking system. Fraudulent transactions were carried out by usage of cloned credit /ATM cards they collect card details and copy the same with the help of a skimmer machine.”<sup>304</sup>

viii. **Plastic Card Fraud:**

“Plastic card fraud is to use a credit or debit card without the knowledge of the card holder to make unauthorized transactions from the victim’s account. In this type of fraud, criminals use the victim’s stolen card in ATM cash machines and try to crack the PIN. In this type of fraud the card and card holder won’t be present physically for the payment. The fraudsters use different modes for obtaining card details such as scam mail, phishing or hacking the victims account.”<sup>305</sup>

“On February 16, 2018 cyber fraud was conducted in Mumbai 30

---

<sup>303</sup>The Hindustan Times dated: 16 November 2019 JRL: <https://www.hindustantimes.com/cities/15-months-later-no-lead-in-rs-94-cr-cosmos-bank-cyber-fraud-case/story-Ar6lk69HLJmBEyt9jGsx0K.html>

<sup>304</sup>Financial Express dated August 20, November 2018 URL: <https://www.financialexpress.com/industry/banking-finance/how-rs-94-crore-online-fraud-was-carried-out-in-punes-cosmos-bank/1286068/>

<sup>305</sup> Hamid Jahankhani, A. Al-Nermrat& Ami Hosseinian- Far, “Cyber Crime Classification and Characteristics,” November 2014, URL: [https://www.researchgate.net/publication/280488873\\_Cyber\\_crime\\_Classification\\_and\\_Characteristics](https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics) (visited on 21.1.2020)

customers of HDFC became victim to cyber fraud resulting in loss of Rs. 10 lakh.<sup>306</sup>

In **Xxx v. State Bank Of India & 2 Ors (2013)**<sup>307</sup> there was an instance of ATM fraud resulting in a loss of monetary value of account holders. The Court held that banks should maintain and follow security protocols in order to prevent ATM frauds in coming days. In **Manager Axis Bank Ltd., v. 1.SaiSandeepBhosle on 22 September; 2017**<sup>308</sup> this was the appeal filed under Section 15 of the Consumer Protection Act by the complainant. The complainant is the account holder bearing No. 912919943689929 under power scheme with the bank. On 01-07-2014 Fraudulent transaction of Rs. 5, 099/- was made from his account after the debit card was under his possession and he did not receive any alert message from the bank. Complainant made a request to the Customer Care to block his debit card and he complained to the bank authority about the unauthorized transaction from his bank account, so bank authority assured him that they will investigate the matter and refund the amount deducted from his account. But till date neither he received any money on his account nor any kind of response from the bank authority. The complainant unblocked his debit card after a month but unfortunately again the amount Rs. 8, 000/- was fraudulently transferred through his card on 8-08-2014. Again he complained to bank authority and subsequently told them the

---

<sup>306</sup>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 Practices, International Journal of Pure and Applied Mathematics, Volume 119 (2018) URL: <https://acadpubl.eu/hub/2018-119-17/2/135.pdf> (visited on 26.8.2019)

<sup>307</sup> Xxx v. State Bank of India & 2 Ors, AIR 2013

<sup>308</sup>Manager Axis Bank Ltd., v. Sai Sandeep Bhosle AIR 2017

unauthorized transaction was made through internet banking. He also informed authority that he has blocked internet banking services there transaction won't be possible through this medium from his account.<sup>309</sup>

After investigation it was found that the above mentioned transaction took place before blocking internet banking. The court held that though his account was closed with the appellants' bank, the fraud was committed while he was the customer/ account holder of the bank and it is their responsibility to find out the details of the fraudster and to take necessary steps in order to get back his money. The court also said that customers/consumers should be very careful while making internet banking transactions. It will be a bank deficiency in service not to take any relevant steps to protect their customer and to get their money from the fraudster even after being aware about the transaction. There is a burden of proof laid down on the bank in case any fraud has occurred on the customers of the bank.<sup>310</sup>

### **3.3. Investigation Mechanism and issues.**

The characteristic of cyber-crime makes cyber fraud different from traditional crime in terms of law enforcement basis, filing investigation, collecting and protecting pieces of evidence, identification of the site, judicial identification, and legal proceedings. "In investigating cyber fraud, there is a high requirement for the officials with professional knowledge, having practical experiences and quality investigators. The investigators need a proper solid foundation of subject knowledge such as

---

<sup>309</sup><https://indiankanoon.org/doc/15001210/>

<sup>310</sup> <https://www.casemine.com/judgement/in/59f95ced4a932658e9ccc2e5>

computer science and technology, keep updating individual time and again about the developments of network technology. They must improve their investigation and enrich their level of technology and tactics.”<sup>311</sup> The law enforcement agencies don't have enough computer literate investigators. There are ample reasons why so few cases are being dealt with; the first is the victims' failure to report cyber fraud. It might be because the victims were unaware that they had been victims of cyber fraud or their computer security had been breached, resulting in the illegal transaction from their account.

Cyber fraud is a type of cybercrime so the two essential elements of crime are present in cyber fraud i.e. *actus reus*<sup>312</sup> and *mens rea*.<sup>313</sup> Every crime must be considered in two parts: the physical act of the crime (*actus reus*) and the mental intent to do the crime (*mens rea*). “In case of cyber fraud it has been challenging to the state to prove *actus reus*. Entire act occurs in the virtual world. It's very tough to collect evidence and submit it in the court. The evidence must be in physical format or in any such other form where it becomes admissible in the court.”<sup>314</sup> *Mens rea* is the other essential element which constitutes crime i.e., ‘a guilty mind’. *Mens rea* is an essential element of crime, with the advent of cyber fraud; one should see the state of mind of a fraudster while conducting the act. An observation at this point worth to be discussed that vulnerability of human being demand laws for their protection<sup>315</sup> similarly, we can say computers and account details of customers are also vulnerable so rule of law is required in order to protect and safeguard them against

---

<sup>311</sup> Wu Yanbo, Xiang Dawei, Gao Jing Ming & Wu Yun, “Research on Investigation and Evidence collection of Cybercrime Cases”, 2018 IOP Con. Series: Journal of Physics: Conf. Series 117 (2019)

<sup>312</sup>*Actus reus* refers to the act or omission that comprise the physical elements of a crime as required by statute

<sup>313</sup>*Mens rea* is a latin term which means “guilty mind”. *Mens rea* refers to the mental element necessary for a particular crime.

<sup>314</sup> Pretty Lather, Cyber Crimes in India and the Legal Regime to Combat it,” Dissertation (Unpublished) submitted to the Faculty of Law, University of Delhi, 2006

<sup>315</sup> *Supra* note at 12



cybercrime.<sup>316</sup>When a hacker, secure access to any device or account he may not all the time aware of where or to which account he is accessing, though his act can direct them to any computer and not to a particular computer. The hackers need not be aware about which computer they exactly were attacking.<sup>317</sup>

With the advancement of technology, the criminal has become more advanced as the criminal's misuse of encryption and the Dark Web has to lead in such a situation where the perpetrator's physical location is no longer found by law enforcement. "There is no common legal framework that exists for the preservation or sharing of evidence. Even though the evidence was preserved for a long period, time may be needed before the evidence is made available for the investigation or judicial proceedings in the requesting country. Since the collection of electronic evidence is often a time-sensitive issue."<sup>318</sup>

In India to investigate the case of cyber fraud, the Sub-Inspector rank of an official is being appointed. But those officers are simply graduate pass-outs who do not have any specialized expertise in particular subject matters, which make them incapable of dealing with present-day crimes like cyber fraud. As to prevent and control, the cyber fraud department must set up a separate investigation agency appointing highly intelligent officials specializing in subjects like computer forensic and information technology. Cyber fraud is a high tech crime, so it is necessary to have high-tech detection techniques in the investigating agency. The department must continuously

---

<sup>316</sup>Sarah Gordon, Richard Ford, "On the definition and classification of cybercrime," March 2006 URL: <http://index-of.es/Viruses/O/On%20the%20definition%20and%20classification%20of%20cybercrime.pdf>

<sup>317</sup>*Supra* note at 10

<sup>318</sup>Joint Report Europol and Eurojust Public Information June 2019 URL: [http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20\(June%202019\)/2019-06\\_Joint-Eurojust-Europol-report\\_Common-challenges-in-combating-cybercrime\\_EN.PDF](http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF)

upgrade its investigative equipment, and officials must be provided with continuous skill training and update the present technology. Even there is a requirement for cyber fraud "investigation measures."<sup>319</sup> Cyber fraud is complicated to investigate but it's even more challenging to gather evidence and try to arrest the culprit. The task of investigating electronic evidence for cyber fraud must need utmost care and caution for file being deleted, overwritten, virus corrupting the file, disk getting formatted. The critical data need extra caution for the protection of data from getting deleted, formatting or stopping it from getting corrupted.<sup>320</sup>

The conviction rate of cyber fraud is shallow. Therefore, combining the characteristic and law of cybercrime, improving investigation techniques and methods is key to detecting such cases. To control or overcome the issues of cyber fraud there is a need for a mutual legal assistant in legal systems and coordination along with the involvement of judicial authorities among the countries for collecting electronic evidence for judicial proceedings. "There are many aspects of cyber fraud which make investigations more difficult for investigating authority. The first aspect is the geographic location since it takes place over multiple regional or national jurisdictions, where it requires international collaboration."<sup>321</sup>

The investigation authority of cyber fraud cannot rely upon the raw evidence rather than the standard form of digital evidence. **R v. Cochrane**,<sup>322</sup> the case is considered as the landmark case for standard form of electronic evidence . In this case printout

---

<sup>319</sup> Investigative measures refer to specific means of investigation

<sup>320</sup>Seokhee Lee, Hyunsang Jun, Aangjin Lee, Jongin Lim, Digital evidence collection process integrity and memory information gathering, Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop Volume, Issue-7-9 November

<sup>321</sup> Dr. Hayes Ben, Dr. Jeandesboz Julien, Dr. Ragazzi Francesco, Dr. Simon Stephanie & Mitsilegas Valsamis, "The Law enforcement challenges of cybercrime: are we really playing catch-up" , October 2015 URL:

[https://www.researchgate.net/publication/283481769\\_The\\_law\\_enforcement\\_challenges\\_of\\_cybercrime\\_are\\_we\\_really\\_playing\\_catch-up](https://www.researchgate.net/publication/283481769_The_law_enforcement_challenges_of_cybercrime_are_we_really_playing_catch-up) visited on 5/11/2019

<sup>322</sup> R v. Cochrane, 1993, United Kingdom

for computers from the Automated teller machine is considered to be the authenticated, standard and direct or real digital evidence. The investigator of digital forensic specialist should possess technical ability to acquire and process the document i.e., electronic evidence.

### **3.3.1. Electronic or Digital Evidence:**

Digital evidence is information collected from the computer during the investigation which is stored, received, or transmitted by the man made electronic device such as computer system, pen drive, USB etc.<sup>323</sup> “Electronic evidence is not similar to traditional evidence such as paper documents, fingerprint, medical report, hand writing, murder weapon, etc.”<sup>324</sup> “The data stored in a computer is considered digital because it is found in cryptography or code form.”<sup>325</sup> Electronic evidence must be evaluated by experts as it is very risky it might get deleted if acted recklessly. Agencies do not have digital evidence experts, and on the other hand, if they do, then the officer might be a specialist particularly in cell phones but not in bank fraud.”<sup>326</sup>

Electronic/ digital evidence is a rapidly growing phenomenon, and courts have little experience or capacity to deal with it. Digital evidence is volatile and fragile; the improper handling of this evidence can alter it. Data is stored on digital devices such as computers, smart phones, tablets, external storage

---

<sup>323</sup> “Electronic Crime Scene Investigation: A Guide For First Responder”, 2<sup>nd</sup> Edition, National Institute of Justice, April 2008

<sup>324</sup> Dr. Nidhi Saxena & Dr. Veer Mayank, “Forensic Hurdles in Investigation & Prosecuting Cyber-crime- An Overview”, The Indian Police Journal

<sup>325</sup>A Simple Guide to Digital Evidence URL: Microsoft Word - digital.docx (forensicsciencesimplified.org)

<sup>326</sup>A Simple Guide To Digital Evidence, URL: <http://www.forensicsciencesimplified.org/digital/DigitalEvidence.pdf> (visited on 22/2/2020)

devices (hard drive, USB device), network components and devices (routers), server, and the cloud data centers in different geographic locations.<sup>327</sup>

In **Anvar P. V v. P. k. Basheer & Ors (decided on 18 September, 2014)** is a landmark case for digital evidence. The Supreme Court noted that there is a revolution in the way that evidence is produced before the court. The Supreme Court held that Section 65A and 65B create some special provisions which override the general law of documentary evidence. So now, all the conditions as listed under section 65B must be satisfied and a certificate be taken to make an evidence admissible.<sup>328</sup>

In **Abdul RahamanKunji v. State of West Bengal (decided on 14.11.2014)**<sup>329</sup> the Hon'ble court of Calcutta dealing with admissibility of email as evidence. The court held that if an email is downloaded or even a print of the same has been taken then both the download and print of such an email is admissible under Section 65B and Section 88A of Evidence Act. The testimony of the witness while carrying out such a document (download and print) the same applies with the electronic communication as evidence in court proceedings.

Electronic evidence, compared to traditional evidence, poses technical unique authentication challenges before investigating authority because of the volume of present data and its velocity,<sup>330</sup> volatility,<sup>331</sup> and its fragility. Currently, “the

---

<sup>327</sup>Digital Evidence 2019 (March) URL: <https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html> (visited on 3/5/2019)

<sup>328</sup> Digital Evidence Law India and all Anvar v Basheer URL: Digital Evidence Law India (cyberblogindia.in)

<sup>329</sup>Abdul Rahaman Kunji vs The State Of West Bengal on 14 November, 2014 (indiankanoon.org)

<sup>330</sup>.Velocity means the speed with which it is created and transferred. See: <https://www.thoughtco.com/velocity-definition-in-physics-2699021>

majority of crimes have a digital component; it duplicates the quality of digital evidence stored for a period of 18- 20 months.”<sup>332</sup> The investigating official or police must collect, preserve, and adequately distribute the electronic evidence before the court.

“The limitation regarding electronic or digital evidence is first, due to the encryption<sup>333</sup> it requires decoding before data can even be accessed.<sup>334</sup> Secondly, there technical and legal are both legal and technical limitations in the investigation of cyber fraud. Cyber fraud is digital crimes that can easily cross-jurisdiction, making standardization and increasingly significant law enforcement issue. The Supreme Court in **State v. Mohd. Afzal and Ors**<sup>335</sup> held that electronic records generated via computer are admissible before court of law if proved in the manner specified by the Section 65B of Indian Evidence Act.

### 3.3.2. Collection of electronic evidence :

In the process of detecting cyber fraud, it is crucial to implement computer forensics and fix crime evidence. "To ensure authenticity before court for electronic evidence, they must focus on collecting electronic evidence according to the law. They must strictly appoint electronic experts for

---

<sup>331</sup>Volatility means it can quickly disappear by being overwritten or deleted. See: <https://www.investopedia.com/terms/v/volatility.asp>

<sup>332</sup>Rodrigue Glen Dario & Molina Fernando, “ The Preservation of Digital Evidence and Its Authority in the Court,” January 2017, URL: [https://www.researchgate.net/publication/312665626\\_The\\_preservation\\_of\\_digital\\_evidence\\_and\\_its\\_admissibility\\_in\\_the\\_court](https://www.researchgate.net/publication/312665626_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court) (visited on 28/4/ 2019)

<sup>333</sup> Encryption is the process to convert information or data to the Code.

<sup>334</sup> *Supra* note at 305

<sup>335</sup> (2003) DLT 385, 2003 (71) DRJ 17

investigation and even ensure the privacy rights of the parties.”<sup>336</sup> During the whole process of investigation it is very difficult to maintain the integrity of electronic evidence

### **3.3.3. Extraction of electronic evidence:**

In cyber fraud, the primary source of electronic evidence is stored on computers, so the extraction of computer evidence can also be considered the computer forensic analysis in the process of finding valuable data from computer systems. While extracting computer evidence, they must consider certain principles:

- a. They must maintain the originality of the computer data. Because of the forensic analysis of the data is a process of copying the data from the original bitstream.
- b. They must ensure the continuity of evidence after submitting it before the court. Since there won't be any changes in electronic evidence, in case of a change in evidence, they must be able to explain the change from the initial to the state of appearance before the court.
- c. They must maintain the integrity of the data during analysis and delivery.

---

<sup>336</sup>Ekaterina A. Drozdova, “Civil Liberties and Security in Cyberspace,” Chap. 5 of this volume URL: [https://www.hoover.org/sites/default/files/uploads/documents/0817999825\\_183.pdf](https://www.hoover.org/sites/default/files/uploads/documents/0817999825_183.pdf) (visited on 9/12/2019)

- d. The accreditation of the forensic process. All the investigation process of obtaining computer evidence must be done under the supervision of experts, appointed by the authority.
- e. In collecting cyber fraud evidence, it is necessary to restore the destroyed and deleted electronic data in time (before it too late) and in an accurate manner.

#### **3.3.4. Maintaining privacy of Individual:**

In cases of cyber fraud, measures to protect information systems from cyber attacks are receiving more attention. But while evaluating specific measures of cyber fraud, legal principles are applicable, such as the right to privacy, unwarranted searches, and seizures. There is a problem protecting public safety and order by law enforcement.<sup>337</sup> In investigating cyber fraud or collecting electronic evidence, there is a chance of intruding into individual privacy rights. India is a signatory to the “Universal Declaration on Human Right.”<sup>338</sup> (UDHR) and “the International Convention on Civil and Political Right”<sup>339</sup> (ICCPR) both of the Convention recognize privacy as a fundamental right. Although being a member and signatory of UDHR and ICCPR conventions, India does not have a law which guarantees the right to privacy to its citizens. “To overcome this lacuna in the law, the Courts in India tried to enforce the

---

<sup>337</sup> Chapter 5 Civil liberties and Security in CyberSpace, Ekaterina A. Drozdova, URL: [https://www.hoover.org/sites/default/files/uploads/documents/0817999825\\_183.pdf](https://www.hoover.org/sites/default/files/uploads/documents/0817999825_183.pdf)

<sup>338</sup>Article 12 of Universal Declaration of Human Rights: No one shall be subjected to arbitrary interference with his privacy family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

<sup>339</sup>Article 17 of ICCPR: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.  
2. Everyone has the right to the protection of the law against such interference or attacks."

right to privacy of its citizens through recognition of constitutional “right to privacy”<sup>340</sup> Which has been read as part of the "rights to life and personal liberty"<sup>341</sup> as well as the “freedom of expression and movement”<sup>342</sup> guaranteed by Indian Constitution. “Privacy in India has been protected through a combination of constitutional and legislative instruments.”<sup>343</sup> The right to privacy was first noticed by constitutional principle in India by the Supreme Court in 1962 in the case of *Kharak Singh v. Union of India*.<sup>344</sup> In cases of cyber fraud in banks involves the protection of consumers from unlawful access to their accounts, sharing, or disclosure of their account information.

### 3.3.5. Search and seizure of electronic evidence:

Section 93<sup>345</sup> of the Criminal Procedure Code, 1973 mandates for a magistrate to issue a search warrant for any document or thing and also

---

<sup>340</sup>According to Black Law Dictionary, Privacy means "right to be let alone; the right of a person to be free from unwarranted publicity; and the right to live without unwanted interference by the public in matters in which the public is not necessarily concerned".

<sup>341</sup>Article 21 of Constitution of India: No person shall be deprived of his life and personal liberty except according to procedure established by law.

<sup>342</sup>Article 19 of Constitution of India: Protection of certain rights regarding freedom of speech, etc.-(1) All citizens shall have the right-

- (a) to freedom of speech and expression;
- (b) to assemble peaceably and without arms;
- (c) to form associations or unions;
- (d) to move freely throughout the territory of India;
- (e) to reside and settle in any part of India's territory; and to practice any profession, or to carry on any occupation trade or business.

<sup>343</sup>*Supra* note at 317

<sup>344</sup> 1963 AIR 1295, 1964 SCR (1) 332

<sup>345</sup> When search warrant may be issued: (1)(a) Where any Court has reason to believe that a person to whom a summons or order under section 91 or a requisition under sub-section (1) of section 92 has been, or might be, addressed, will not or would not produce the document or thing as required by such summons or requisition, or

(b) where such document or thing is not known to the Court to be the possession of any person, or  
(c) where the Court considers that the purposes of any inquiry, trial or other proceeding under this Code will be served by a general search or inspection,

it may issue a search-warrant; and the person to whom such warrant is directed, may search or inspect in accordance therewith and the provisions hereinafter contained.



warrant for general search in the area only for the purpose of investigation. Other Sections 165<sup>346</sup> and 51<sup>347</sup> provide for search without a warrant if any officer in charge feels that it would be time consuming in acquiring a warrant and the evidence shall be lost then the officer can search the premises without a warrant. In **Swaran Sabharwal v. Commissioner of Police, 1998 Criminal Law Journal 240**<sup>348</sup> the court held that police officers could issue a direction to various banks for freezing the account. Therefore, like any other property bank account is freezable under section

---

(2)The Court may, if it thinks fit, specify in the warrant the particular place or part thereof to which only the search or inspection shall extend; and the person charged with the execution of such warrant shall then search or inspect only the place or part so specified.

(3)Nothing contained in this section shall authorise any Magistrate other than a District Magistrate or Chief Judicial Magistrate to grant a warrant to search for a document, parcel or other thing in the custody of the postal or telegraph authority.

<sup>346</sup> Section 165 Criminal Procedure Code, 1973: Search by police officer- (1) Whenever an officer in charge of a police station or a police officer making an investigation has reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorised to investigate may be found in any place within the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his opinion be otherwise obtained without undue delay, such officer may, after recording in writing the grounds of his belief and specifying in such writing, so far as possible, the thing for which search is to be made, search, or cause search to be made, for such thing in any place within the limits of such station. (2) A police officer proceeding under sub-section (1), shall, if practicable, conduct the search in person. (3) If he is unable to conduct the search in person, and there is no other person competent to make the search present at the time, he may, after recording in writing his reasons for so doing, require any officer subordinate to him to make the search, and he shall deliver to such subordinate officer an order in writing, specifying the place to be searched, and so far as possible, the thing for which search is to be made; and such subordinate officer may thereupon search for such thing in such place. (4) The provisions of this Code as to search-warrants and the general provisions as to searches contained in section 100 shall, so far as may be, apply to a search made under this section. (5) Copies of any record made under sub-section (1) or sub-section (3) shall forthwith be sent to the nearest Magistrate empowered to take cognizance of the offence, and the owner or occupier of the place searched shall, on application, be furnished, free of cost, with a copy of the same by the Magistrate.

<sup>347</sup> Section 51 of Criminal Procedure Code, 1973: Search of arrested person- (1) Whenever a person is arrested by a police officer under a warrant which does not provide for the taking of bail, or under a warrant which provides for the taking of bail but the person arrested cannot furnish bail, and whenever a person is arrested without warrant, or by a private person under a warrant, and cannot legally be admitted to bail, or is unable to furnish bail, the officer making the arrest or, when the arrest is made by a private person, the police officer to whom he makes over the person arrested, may search such person, and place in safe custody all articles, other than necessary wearing-apparel, found upon him and where any article is seized from the arrested person, a receipt showing the articles taken in possession by the police officer shall be given to such person. (2) Whenever it is necessary to cause a female to be searched, the search shall be made by another female with strict regard to decency.

<sup>348</sup> 1990 68 Comp Cas 652 Delhi

102 Cr PC<sup>349</sup>. Freezing the account is an act in the investigation. It will preserve the secrecy of least valuable evidence. The process of search and seizure of electronic evidence is the present challenge for cyber police.

### 3.3.6. Challenges during electronic investigation:

New phase of digitalization has created new areas of challenges as well as opportunities for investigation. Bank shafting its way of traditional banking towards internet banking has created new systems/methods of providing their services before their customers. These channels proved to be sufficient and acceptable mediums to the consumer from the worldwide. All these created paperless transactions of money via online banking using varieties of mobile applications such as Bhim App, Paytm, Google pay, Paypal etc. Information Communication Technology developed a new updated security system considering the customer security and interest but with advancement of technology system predators has also become smarter which makes them two steps ahead of security systems. They are looking for a new modus operandi for conduct of fraud in the banking system.

The predators are misusing the services by cheating or conducting fraud by manipulating customers. They are creating scam by sending bug messages

---

<sup>349</sup>Power of police officer to seize certain property: (1) Any police officer may seize any property which may be alleged or suspected to have been stolen, or which may be found under circumstances which create suspicion of the commission of any offence.

(2) Such police officer, if subordinate to the officer in charge of a police station, shall forthwith report the seizure to that officer.

[(3) Every police officer acting under sub-section (1) shall forthwith report the seizure to the Magistrate having jurisdiction and where the property seized is such that it cannot be conveniently transported to the Court, he may give custody thereof to any person on his executing a bond undertaking to produce the property before the Court as and when required and to give effect to the further orders of the Court as to the disposal of the same.]

via emails or text messages and sometimes by voice call posing to be officers from the institute. Cyber fraud involves many parties; it makes it difficult and sometimes even more impossible to indicate the exact place of offence. “In the early days, the ability of law enforcement in order to carry out investigation of computer technology was limited because of the lack of expertise in computer forensic.”<sup>350</sup> Collection of digital evidence is very important in cyber fraud investigation. It's very relevant to identify digital evidence in time so that investigating authorities can collect and preserve it in a secure manner, later they can use the evidence before court proceedings. In order to reach the digital evidence there is need for “computer forensic”<sup>351</sup> expertise. “Computer Forensics involves evaluating the data by using different methods. It helps in investigating electronic evidence.”<sup>352</sup> Individuals not being expertise won't be able to crack the investigation as we there required a specific procedure to collect the digital evidence.

The process of investigating digital evidence or seize evidence and presenting them before court proceeding are not limited within the traditional methods. Technology has made an influence in people's life, and digital evidence has become an important source of evidence even for

---

<sup>350</sup>Whitecomb Carrie Morgan, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Spring 2002 Vol. No. 1, Issue 1 URL: <https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf> (visited on 10.4.2020)

<sup>351</sup>Computer Forensic is a branch of digital forensic science encompassing the recovery, investigation and analysis techniques in order to collect and preserve electronic evidence particularly from computing devices so later on they can present it before the court of proceedings. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

<sup>352</sup> URL: <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> visited on (22.4.2020)

conventional crime. The reason for the challenges is that apart from similarities there are major differences among the evidence. The basic requirements for the evidence are that they must be authentic, reliable, complete and accurate with the legal requirements. Electronic evidence is a new category of evidence; it's based on scientifically reliable principle and procedure. Now there is a need for establishment of more scientific research and training centers in India in different states. Investigation of electronic evidence involves technicalities, just being a Sub-Inspector, or investigating officials isn't enough for the analysis of the data or evidence. The experts are required for analyzing and evaluating digital and should possess a special skills, technical understanding which are not necessarily covered by the professionals such as judges, lawyers, legislators, police etc. They therefore, require experts for recovering, collecting and analyzing digital evidence. Those officials of cyber police teams must have all the required subject qualification to avoid uncertainty. Another challenge while collecting digital evidence is the nature of digital evidence. Electronic computer data is easily deleted or modified because of its fragile nature it can be easily tempered by the fraudster. "The collection of digital evidence always involves certain technical requirements; to avoid the losses of data it requires some technical measures. To preserve and protect the integrity of digital evidence for a long period of time, are achieved.<sup>353</sup> Before handling digital evidence, it requires standard procedure in order to maintain the effective system. In

---

<sup>353</sup>Hosmer Chet, Proving the Integrity of Digital Evidence with the Time, International Journal of Digital Evidence Spring 2002 Vol.1, Issue 1 URL: <https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf> (visited on 4.4.2020)

order to present digital evidence before the courtroom, there required some infrastructure that needs to be installed such as a screen which is very important to be there in the courtroom to ensure that judges, prosecutors, defence lawyers, the accused along with other jury present will in order to follow the presentation of evidence. Till date our courtroom is enough to have traditional proceedings but admissibility of digital/electronic evidence seeks the authority for the installation and maintaining such equipment and this will generate a significant cost for the judicial system which they need to provide. Technology has been constantly changing, this required for the constant review of the procedures and providing required training in order to ensure stability and effectiveness during investigation. With time, new versions of software and operating systems will always keep on creating challenges.

#### **3.4. Prosecuting issues.**

All the crimes in society have considerable attrition, which is being perpetrated against us. The numbers of cases of cyber fraud that occur are large in numbers. Still, the actual number of cases reported to the police or other official agencies for investigation and the number of cases resulted in judicial proceedings and punishment for the offenders are very less. Banking Institution started cashless banking services in order to foster transparency, curb corruption and convenient banking to their customers but it has started growing fraudsters of fraud and a major question of safety has arisen before the bank, legislature and judiciary. Cyber fraud being a hi-tech crime involves multiple parties making it difficult to track the fraudster and their location. The conviction of accused in cases of cyber fraud is very

low even though 75% of the cyber crime constitutes cyber fraud. “As per information from home ministry data 2016, in 2015, 11592 cases were registered across the country and 3206 charge sheet was filed out of which conviction was only in 234 cases. In 2014 9622 cases were registered and only 76 convictions were there.”<sup>354</sup> Almost every year the cases of cyber crime is getting doubled and prosecuting procedure is getting slower. Indian cyber law i.e. Information Technology Act, 2000 consider as it covers all the cyber crimes and provides punishments but the cyber terrorism is only punishable with life imprisonment and the rest of other offences are just punishable up to three years along with fine. Now if we look into the present scenario we can clearly figure out that cyber frauds are getting more dangerous and it's making the situation worse. Judiciary can't overlook cyber fraud; it is the high time to act in order to control the situation. They need to amend the IT Act, 2000 providing a specific section that covers cyber fraud by including its definition along with punishment. Lack of provided definition or the parameter constituting cyber fraud is one of the prime obstacles for prosecuting procedure. “In absence of a well-established collaboration among the countries about sharing the information with other countries are lacking uniform law, there are inadequate laws to combat cyber fraud. Due to the lack of standard procedure of search seizure and analysis of electronic evidence less numbers of convictions in cyber fraud are taking place.”<sup>355</sup> The law is silent in providing procedures for conducting search and seizure in cyber fraud and they have not provided any documented procedure in order to perform searching and seizing digital evidence and procedure operating forensic examination of digital evidence.

---

<sup>354</sup>Cyber Crime: Are The Law Outdated in India For This Type of Crime? URL: <http://www.legalserviceindia.com/legal/article-2454-cyber-crime-are-the-laws-outdated-in-india-for-this-type-of-crime-.html> (visited on 24/9/2020)

<sup>355</sup>Why most cybercrimes in India don't end in conviction (livemint.com)

Cyber fraud being a borderless crime involves many jurisdictions. Investigating officials even after performing excellently remained unsuccessful in cracking the case; it got beyond the country boundaries. The procedure that they need to follow leads to delaying in tracing the accused because they have to obtain court orders for investigating in other jurisdictions following Mutual Legal Assistance (MLA) signed between India and other countries for providing legal assistance during investigating procedure. All these processes lead to cases stagnant for months within which accused can even tampered with the electronic evidence which is of fragile nature. Thus the cyber fraud cases are growing where fraudster are very confident about their conviction not being possible in absence of strict cyber law with severe punishment

“Data Security Council of India (DSCI) was started by the software industry group NASSCOM in order to promote data protection. Data Security Council of India provides special learning sessions for those departments.”<sup>356</sup> The government of India is investing on the training but government officials don't have the knowledge of their power under the Information Technology Act, 2000, they are unable to adjudicate their powers. This is creating delay for prosecuting the case before the court.

### **3.5. Issues of Consumer Liability.**

“Consumer liability places consumers accountable for the negligence on their part while performing banking activities.”<sup>357</sup> “Customers are responsible for keeping his/her account details such as ATM card, PIN number, internet banking username and password, mobile banking details safe. Internet banking is making benefits for both banks and customers. The problem that occurs is the security issues of their

---

<sup>356</sup>Why most cybercrimes in India don't end in conviction. URL: <https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html> (visited on 10/8/2020)

<sup>357</sup> <https://www.investopedia.com/terms/c/consumer-liability.asp>

customers. When a customer discovers fraudulent transactions from their account and even after making reporting to banking authorities they are not taking any action for the investigation and providing relief to the customers. Bank will be held responsible for the fund that they lost and the bank must take entire responsibility for the loss. India's central banking institution is the Reserve Bank of India (RBI) which works for the protection of banking customers and provides guidelines for providing security and regulation in order to regulate banking institutions properly.”<sup>358</sup>

The Reserve Bank of India has issued guidelines limiting consumers' liability in case of unauthorized transactions that take place from mobile wallets. As per guidelines, Prepaid Payment Instrument (PPI)<sup>359</sup> issuers will be required to provide a contact number or email ID in the transaction alert SMS through which consumers can report the unauthorized transaction.

Prepaid Payment Instrument is issued under three types<sup>360</sup>:-

“a). **Closed System PPIs:**

Close System Prepaid Payment Instruments are issued for the purchasing goods and services but cash withdrawals are not permitted. The Closed System of payments instrument is not allowed to be used for the third party payment. The operation of

---

<sup>358</sup>Customers' Liability in Age of Digital Banking URL: <https://www.finextra.com/blogposting/14308/customer-liability-in-the-age-of-digital-banking>

<sup>359</sup> In exercise of the power conferred under Section 10(2) of the Payment and Settlement System (PSS) Act, 2007, Reserve Bank of India has issued the direction of Prepaid Payment Instruments (PPI). PPIs are instruments that facilitate (a) purchase of goods and services, including financial services, (b) remittances, (c) funds transfers, etc. Prepaid instruments can be issued as smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, paper vouchers.

<sup>360</sup>Prepaid Payment Instrument (PPIs) URL: [https://m.rbi.org.in/scripts/FS\\_FAQs.aspx?Id=126&fn=9](https://m.rbi.org.in/scripts/FS_FAQs.aspx?Id=126&fn=9)



such an instrument is classified as a payment system and it does not require any approval or authorization from the reserve Bank.”<sup>361</sup>

**b). Semi- closed System PPIs:**

“Semi-closed System instruments are only issued with the approval of the Reserve Bank of India and non-bank to purchase goods and services, they also provide financial services with specific contracts. This instrument has not allowed cash withdrawal as they are issued by the Banks or non-banks.”<sup>362</sup>

**c). Open System PPIs:**

With the approval of the Reserve Bank of India, ‘Open System Instruments are issued by banks to purchase goods and services. Certain services like cash withdrawal at ATMs etc. are permissible over these PPIs.”<sup>363</sup> For providing better services to customer and protection to Indian banks Reserve Bank of India (RBI) works on limited customer liability. RBI has provided notification for “**Consumer Protection- Limited Liability of Customers in Unauthorised Electronic Banking Transaction.**” RBI has divided electronic banking transaction into two categories

i.“Online payment where physical presence is not required it can be done via, internet banking, mobile banking.

ii. Physical presence of a card is needed e.g. ATM etc.<sup>364</sup>

---

<sup>361</sup>Reserve Bank of India - FAQs (rbi.org.in)

<sup>362</sup> *Supra* note at 362

<sup>363</sup> *ibid*

<sup>364</sup> Consumer Protection- Liability of Customers in Unauthorised Electronic Banking Transaction URL: Reserve Bank of India - Notifications (rbi.org.in)

The bank in order to provide better system and ensure processes safely and security of electronic transaction RBI has made mandatory to all banks to follow certain rules:-

- a. They must ask Customers to register their telephone number or email id in banks in order to receive SMS alerts in case of unauthorized electronic transactions.
- b. Banks must send text alerts messages to customers for all electronic transactions as well as email alerts to customers on their registered email.
- c. Banks must have separate departments for receiving complaint reports of unauthorized transactions 24 x 7 through multiple channels such as bank websites, phone banking, toll-free helpline, SMS, email, IVR.
- d. Banks must instantly respond to the complaint filed by a customer by text alert for unauthorized transaction.

Reserve Banks have provided that customers have **zero liability fraudulent payment** occurs in case of:-<sup>365</sup>

- i. In case of contributory or negligence fraud of banks are held liable irrespective of whether transactions are reported or not by their customers.
- ii. Banks will be held liable if the unauthorized transaction has caused the failure of the system and not by any of the party and within three day inform authority about fraudulent transactions.

---

<sup>365</sup>RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017 dated: July 6, 2017 URL: <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11040>

“Reserve Bank of India has provided limited liability for customers where they will be liable for fraudulent transactions”<sup>366</sup> on following circumstances:-

- i. “In cases where the loss is caused due to the negligence of the customer, where he shared the payment details, customers have to take responsibility for entry unless they report to bank and after making reporting the it is the bank 's responsibility to control the loss and if again such transaction occur than it will be their responsibility.
- ii. If the loss is caused due to technical failure and if customers fail to notify bank in time than it will be their mistake and have to pay half of the transaction amount.”<sup>367</sup>

The burden to prove customer liability always lies with the bank in case of unauthorized electronic banking transactions.

### **3.6. Transnational Issues**

“Cyber fraud has a high potential to create a high impact on the banking institution. Adoption of digitalization of banking made it easy to commit cyber fraud without any physical existence.”<sup>368</sup> Cyber fraud is a hi-tech faceless crime which cannot be limited within national boundaries. Cyberspace and computers do not recognize national boundaries nor does cyber fraud recognize it. Jurisdiction in the cases of cyber fraud and other cyber crime offences is always a debatable one. In cyber fraud there is an involvement of many parties from different countries beyond our national boundaries

---

<sup>366</sup>policy-for-customer-protection-for-limiting-liability-of-customers.pdf (canarabank.com)

<sup>367</sup>RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017 dated: July 6, 2017 URL: <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11040>

<sup>368</sup>Poonia Dr. Ajeet Singh, Cyber Crime: Challenges and its Classification, International Journal of Emerging Trends & Technology in Computer Science Volume 2, Issue 6, November-December 2014 URL: <https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf> (visited on 21/8/2020)

(outside our jurisdiction). Offenders may be from other nations that make challenges to the authorities and regulation to carry forward with the case in other nations.

Thus, the prime transnational issues faced in case of cyber fraud is related to investigation. The investigator while investigating the cyber fraud needs to resort the investigation outside their national boundaries and it's important that each investigating official handling cyber fraud must possess the requisite knowledge of international investigation as prescribed by the law mandated by the government of the particular country. Investigating authority has an important role in collecting evidence so they must be expertise in tracking or collecting the digital evidence. Any police officer after attending training can't be considered to be experts overnight for this issue.

### **3.6.1. Legal Provisions to collect information from outside India**

“In order to gather information from outside India the legal procedure of Mutual Legal Assistance Treaty (MLAT) and ‘Letter Rogatory’<sup>369</sup> or letter of request, guidelines are issued by the Ministry of Home Affairs, Government of India.”<sup>370</sup>

---

<sup>369</sup>Letter Rogatory are the customary means of obtaining judicial assistance from overseas in the absence of a treaty or other agreement. It is a formal communication in writing sent by the Court in which action is pending to a foreign court or judge requesting the testimony of a witness, residing within the jurisdiction of that foreign court, may be taken under its direction and transmitted to the issuing court making request for use in a pending legal contest or action. In case of Union of India v. Chandha (WN) 1933 Cri LJ 859 (SC) a letter of rogatory was issued with request to authorities in Switzerland, for freezing certain bank accounts, and the accused did not claim, any amount connected with Bofors case as being deposited in his Swiss Bank, held that it cannot be said that the accused was deprived of his property and that he is not entitled to any prior notice and opportunity of being heard. See: <http://www.cbi.gov.in/interpol/invletterrogatory.php>

<sup>370</sup>Cyber Crime Investigation Manual, Data Security Council of India, Delhi URL: [https://jhpolicen.gov.in/sites/default/files/documents-reports/jhpolicen\\_cyber\\_crime\\_investigation\\_manual.pdf](https://jhpolicen.gov.in/sites/default/files/documents-reports/jhpolicen_cyber_crime_investigation_manual.pdf)

Section 166A of Criminal Procedure Code, 1973: Letter of request to competent authority for investigation in a country or place outside India- (1) Notwithstanding anything contained in this Code, if, in the course of an investigation into an offences, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India, any Criminal Court may issue a letter of request to a Court or an authority in that country or place competent to deal with such request to examine orally any person supposed to have knowledge about the situation and to record his statement made in the course of such examination and also to require such person or any other person to produce any document or thing which may be in his possession pertaining to the case and to forward all the evidence so taken or collected or the authenticated copies thereof or the thing so collected to the Court issuing such letter.

(2) The letter of request shall be transmitted in such manner as the Central Government may specify in this behalf.

(3) Every statement recorded or document or thing received under sub-section (1) shall be deemed to be the evidence collected during the course of investigation under this chapter.

Section 166B of Criminal Procedure Code, 1973: Letter of request from a country or place outside India to a Court or an authority for investigation in India- (1) Upon receipt of letter of request from a Court or an authority in a country or place outside India competent to issue such letter in that country or place for the examination of any person or production of any document or

thing in relation to an offence under investigation in that country or place, the Central Government may, if think fit-

(i) forward the same to the Chief Metropolitan Magistrate or Chief Judicial Magistrate or such Metropolitan Magistrate or Judicial Magistrate as he may appoint in this behalf, who shall thereupon summon the person before him and record his statement or cause the document or thing to be produced, or

(ii) send the letter to any police officer for investigation, who shall thereupon investigate into the offence in the same manner, as if the offence had been committed within India.

(2) All the evidence taken or collected under sub-section (1), or authenticated copies thereof or the things so collected, shall be forwarded by the Magistrate or police officer, as the case may be, to the Central Government for transmission to the Court or the authority issuing the letter of request, in such manner as the Central Government may deem fit.

In order to conduct formal investigation and collect digital evidence, material object and documents Letter of rogatory/ letter of request are sent through competent Court Section 166A of Criminal Procedure Code, 1973.

### **3.7. Jurisdictional Issues:**

Territorial boundaries do not exist in the virtual world and cyberspace being single devoid of any national boundaries. This global medium has transformed the world into one single community. Cyber fraud is impossible to be limited within national boundaries, since it is committed in many jurisdictions at the same time. It becomes

difficult, sometimes even impossible to conduct investigation due to inaccessible jurisdiction. It won't be wrong to say that cyber fraudsters are here anywhere and everywhere. The jurisdiction issue is highly debatable due to the expanding nature of cyber fraud.<sup>371</sup> Laws applicable to traditional crime are not completely applicable in present digital crime. The involvement of multiple numbers of people, raising serious concern regarding the jurisdiction. Information Technology Act, 2000 stands to be the cyber law for India appears to be inefficient unless its provision is updated considering all the issues of the cyber world. Information Technology Act, 2008 (amendment Act 2008) both are silent in case of jurisdiction issues.

None of the substantive or procedural laws seeks to define the term “Jurisdiction”. Black’s Law Dictionary defines “Jurisdiction” as “A court’s power to hear the case.”<sup>372</sup> Jurisdiction means “the authority of a court and official organization for to making decisions and judgments.<sup>373</sup> “It may refer to defining the proper court to bring a particular case where the court has original or appellate jurisdiction over a case.”<sup>374</sup> The term ‘jurisdiction’ describes the limitation of the legal competence of a State or a different regulatory authority to apply and enforce rules on a particular person.

The jurisdiction of a state is the capacity to make and apply the law and to ensure compliance with the laws through executive, administrative, police, or other non-judicial action. Jurisdiction is the court's capacity to decide the case because of uniform cyber law the jurisdiction is creating difficulties while dealing with the

---

<sup>371</sup>Kalra Kush, Emergence of Cyber Crime: A Challenge for the New Millennium, Bharati Law Review, April- June 2017 URL: <http://docs.manupatra.in/newslines/articles/Upload/4730150C-4A12-4EBA-8CAF-F1146FDD5657.pdf> (visited on 27/8/2020)

<sup>372</sup> Black’s Law Dictionary 10<sup>th</sup> Edition also see FInal-Matter.pdf (cybertalkindia.com)

<sup>373</sup>. <https://dictionary.cambridge.org/dictionary/english/jurisdiction>

<sup>374</sup> <https://legal-dictionary.thefreedictionary.com/jurisdiction>

subject. The unpredictability nature of cyber fraud jurisdiction is making it more difficult to limit their legal liabilities and inhibits the growth of banking business.”<sup>375</sup>

Jurisdictions are mainly categorized into three mainly as below:-

a). **Subject matter Jurisdiction:**

Power of the court to hear and decide specific cases that can be categorized in a subject matter domain. “It is the power of court to pass judgement for concerning event that occurred within defined territory.”<sup>376</sup> The forum in which a legal dispute is or claims to be filed, ought to have authority to decide the matter pertaining to a specific subject matter or domain. The court judgement which doesn't have subject matter jurisdiction is forever nullity.

b). **Personal Jurisdiction:**

Personal jurisdiction is the authority of the court to hear and decide a case against a particular set of persons. It means a person against whom a case is filed should belong to the territorial jurisdiction in which the forum is situated.

c). **Pecuniary Jurisdiction:**

Pecuniary jurisdiction refers to jurisdiction of the court based on the amount of the claim which is made in the proceeding.

The traditional notion of jurisdiction mainly focuses on the particular place/location of the transaction of dispute that took place to determine their exact jurisdiction to

---

<sup>375</sup>United States and European Union Approaches to Internet Jurisdiction and their Impact on E-commerce URL: <https://www.law.upenn.edu/journals/jil/articles/volume25/issue1/Chen25U.Pa.J.Int%27IEcon.L.423%282004%29.pdf> (visited on 21/5/2020)

<sup>376</sup>[https://en.wikipedia.org/wiki/Subject-matter\\_jurisdiction](https://en.wikipedia.org/wiki/Subject-matter_jurisdiction)



adjudicate the case. In the case of internet transactions it has been conducted over several networks so it does not conform to the exact geographical boundaries. Cyber fraud being a borderless crime it makes difficult to establish the geographical location of the fraudster. Without proper jurisdiction the order or decision of a court will be baseless as well as ineffective. “The traditional approach to the jurisdiction asks the court whether they had jurisdiction.

Since cyber fraud is a borderless crime so the transaction in the cyber world is transmitted more easily across the country. There is no border between the countries for committing any kind of cyber fraud.” “According to the view of Gertrude Stein, the internet is everywhere and can pick the exact location for their presence.”<sup>377</sup> The problem with technology is that it keeps on changing very rapidly at least two steps ahead of the Law. In **SIL Import v. Exim Aides Silk Exporters, 1999 (2) KLT 275 (SC)** the Court recognized that it's time for the judiciary to interpret the statute so that they can cover new relevant changes that technology has brought. <sup>378</sup>

What is meant by Jurisdiction? This has been explained in the case of **Hirday Nath Roy v. RamchandraBarnaSarma**,<sup>379</sup> by (acting) C.J., Mukherhee as under:

“In the order of Reference to a Full Bench in the case of Sukhlal v. Tara Chand, (1950) ILR 33 Cal 68 (FB), it was stated that jurisdiction may be defined to be the power of a Court to ‘decide the cause, to adjudicate and exercise any judicial power in relation to it:’ in other words, by jurisdiction is meant ‘the authority which a “Court has to decide matters that are litigated before it or to take cognizance of matters presented in a formal way for its

---

<sup>377</sup> Digital Equipment Corp. v. Altavista Technology, Inc. 960 F. Supp. 456 (Decided on March 12, 1997) URL: Cybertelecom :: Internet

<sup>378</sup> <https://indiankanoon.org/doc/781024/>

<sup>379</sup> AIR 1921 Cal 34 (FB)

decision.’ An examination of the cases in the books discloses numerous attempts to define the term ‘jurisdiction’, which has been stated to be ‘the power to hear and determine issues of law and fact’ “the authority by which the judicial officers take cognizance of and decide causes”; ‘the authority to hear and decide a legal controversy’ “the power to hear, determine and pronounce judgement on the issues before the Court”; “the power or authority which is conferred upon a Court by the Legislature to hear and determine causes between parties and to carry the judgements into effect”; “the power to enquire into the facts, to apply the law, to pronounce the judgement and to carry it into execution”.<sup>380</sup>

Proceeding further the learned Judge observed:

“This jurisdiction of the Court may be qualified or restricted by a variety of circumstances. Thus, the jurisdiction may have to be considered with reference to place, value and nature of the subject matter. The power of a tribunal may be exercised within defined territorial limits. Its cognizance may be restricted to subject- matters of prescribed value. It may be competent to deal with controversies of a specified character, for instance, testamentary or matrimonial causes, acquisition of lands for public purposes, record of rights as between landlords and tenants. This classification into territorial jurisdiction, pecuniary jurisdiction and jurisdiction of the subject-matter is obviously of a fundamental character.”

---

<sup>380</sup> [https://en.wikipedia.org/wiki/Subject-matter\\_jurisdiction](https://en.wikipedia.org/wiki/Subject-matter_jurisdiction)

In **Chandrabai Bhoir v. Krisnna Bhoir**,<sup>381</sup> the court held that the jurisdiction is an important key where it can go to the root of the case and decide the matter in order to provide justice to the victim. If any court without any jurisdiction passes the order then it becomes nullity and not enforceable by law. In **Mobarik Ali v. The State of Bombay**,<sup>382</sup> the Supreme Court explained that the basis of jurisdiction under Section 2 is the locality where the offence is committed and the corporeal presence of the offender in India is immaterial. When a decree is passed without jurisdiction over the subject-matter or when a suit is brought and determined by the court which is not competent to pass or has no jurisdiction then it is said to be "*coram non judice*."<sup>383</sup> A decree passed by such court will be invalid even in the stage of execution or in proceeding.<sup>384</sup> In **Chief Engineer Hydel project v. Ravinder Nath**<sup>385</sup> Hon'ble Apex Court observed that once the original decree held to be without jurisdiction and hit by the doctrine of *Coram non judice* there would be no question of upholding merely on the ground that the objection was not taken at the initial stages. The case of **Gafar v. Government of Kwara State (2007) 4 N.W.L.R (Pt. 1024) 37**, the court held that the constitution of India has already prescribed the jurisdiction. No court can assume jurisdiction except as prescribed by statute.<sup>386</sup> In **JCB India Ltd. v. Abhinav Gupta decided on 1 September 2010**, jurisdiction issues were raised. The Internet can be accessed by anyone from anywhere within the globe but it isn't the criteria to decide territorial jurisdiction. The adjudicating Officer claimed that he has no jurisdiction to

---

<sup>381</sup> AIR 2009 S.C. 1645 Bom

<sup>382</sup> AIR 1957 S.C. 857

<sup>383</sup> Coram non judice is a Latin Legal Maxim which means "not before a judge".

<sup>384</sup> <http://lawtimesjournal.in/coram-non-judice/>

<sup>385</sup> AIR 2008 SC 1315

<sup>386</sup> Chibuko Raphael Ibekwe, The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provision (2015) Ph. D Thesis submitted to the School of Law, University of Stirling : URL: <https://dspace.stir.ac.uk/bitstream/1893/22786/1/Ibekwe%20PHD%20THESIS.pdf> (visited on 10.09.2020)

decide the matter as business place as well as the place of residence was Haryana. There, the Haryana Court is competent to decide the matter.<sup>387</sup>

Presence of multiple parties involved in the commission of cyber fraud makes it a most complicated task to ascertain the place of commission of crime. Sometime locating the fraudster is another challenge for the investigating authorities.<sup>388</sup> The applicable principle is that countries give power to their established court over its subject within the territorial limit of the country.<sup>389</sup>

Since the court deals cyber fraud cases under Indian Penal Code with the similar offences such as cheating, fraudulently, misrepresentation etc. also Section 2,<sup>390</sup> Section 3<sup>391</sup> and Section 4<sup>392</sup> are also applicable.

“The common law doctrine is that criminal law is primarily territorial.”<sup>393</sup> Both the section 3 and 4 of IPC, 1860 deal with those offences which are committed outside

---

<sup>387</sup> <https://indiankanoon.org/doc/179788397/>

<sup>388</sup> Dhupdale Vivek Y., “Cyber Crime and Challenges Ahead” March 2011 URL: [https://www.researchgate.net/publication/265166983\\_Cyber\\_Crime\\_and\\_Challenges\\_Ahead](https://www.researchgate.net/publication/265166983_Cyber_Crime_and_Challenges_Ahead) (visited on 10/5/2020)

<sup>389</sup> Lord Macmillan in *Campania Naviera Vascongado v. Steamship Cristina* (1938) AC 485

<sup>390</sup> Section 2 of Indian Penal Code stated that “Every person shall be liable to punishment under this Code and not otherwise for every act or omission contrary to the provisions thereof, of which he shall be guilty within [India].

<sup>391</sup> Section 3 of Indian Penal Code: Punishment of offences committed beyond, but which by law may be tried within, India- states that “Any person liable, by any Indian law, to be tried for an offences committed beyond India shall be dealt with according to the provisions of this Code for any act committed beyond India in the same manner as if such act had been committed within India.

<sup>392</sup> Section 4 of Indian Penal Code 1860 mention about the extension of Code to extra-territorial offences- The provisions of this Code apply also to any offence committed by-

- (1) any citizen of India in any place without and beyond India;
- (2) any person on any ship or aircraft registered in India wherever it may be.
- (3) any person in any place without and beyond India committing offence targeting a computer resource located in India.

[Explanation- In this section-

- (a) The word “offence” includes every act committed outside India which, if committed in India, would be punishable under this Code;
- (b) The expression “computer resource” shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000.]

<sup>393</sup> Jurisdiction URL: <http://14.139.60.114:8080/jspui/bitstream/123456789/742/9/Jurisdiction.pdf> (visited on 5/5/2020)

India in the same manner as it has been committed within India. Procedure committed outside India has been mentioned under Section 188<sup>394</sup> of Criminal Procedure Code, 1973.

Generally, the State can investigate crimes on their territory on their terms as their sovereign rights. But law enforcement agencies cannot investigate on the foreign territory without prior permission or a treaty enforced between them. According to Section 20 of CPC,<sup>395</sup> “Indian courts decide their jurisdiction as per the parties residing or at the place of their work irrespective of their residing place or place they stay recently.”<sup>396</sup>

A corporation shall carry on business at its sole or principal office in [India] or, in respect of any cause of action arising at any place where it has also a subordinate office, at such place. “The cyber jurisdiction face problem in following matters:

---

<sup>394</sup>Section 188 of Criminal Procedure Code, 1973- Offence committed outside India- When an offence is committed outside India-

- (a) by a citizen of India, whether on the high seas or elsewhere; or
- (b) by a person, not being such citizen, on any ship or aircraft registered in India, he may be dealt with in respect of such offence as if it had been committed at any place within India at which he may be found:

Provided that, notwithstanding anything in any of the preceding sections of this Chapter, no such offence shall be inquired into or tried in India except with the previous sanction of the Central Government.

<sup>395</sup> Section 20 of CPC: Other suits to be instituted where defendants reside or cause of action arises: Subject to the Limitations aforesaid, every suit shall be instituted in Court within the local limits of whose jurisdiction-

- (a) the defendant, or each of the defendants where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain; or
- (b) any of the defendants, where there are more than one, at the time of the commencement of the suit actually and voluntarily resides, or carries on business, or personally works for gain, provided that in such case either the leave of the Court is given, or the defendants who do not reside, or carry on business, or personally work for gain, as aforesaid, acquiesce in such institution; or
- (c) the cause of action, wholly or in part, arises.

[Explanation]- A corporation shall be deemed to carry on business at its sole or principal office in [India] or, in respect of any cause of action arising at any place where it has also a subordinate office, at such place.

<sup>396</sup>Brinda G. Lashkari, “Issue of Jurisdiction Under Cyber Law in India”, Racolb Legal (April 12, 2016), URL: <http://racolblegal.com/issue-of-jurisdiction-under-cyber-law-in-india/> (visited on 10/5/2020)

i. Cyber jurisdiction related to civil matters

ii. in criminal matters

iii. cyber jurisdiction in international matters.”<sup>397</sup>

“It is said that no person can be arrested, a summons may not be served, police investigation cannot be done, or order for the production of documents may not be executed as per guideline of treaty.”<sup>398</sup> When investigating officers collect digital evidence in other countries beyond their jurisdiction, they are not allowed to take that collected evidence. The State having sovereign power over its territory using its power to investigate and collect their evidence falls within the exercise of their sovereignty rights. When foreign authorities use their power over other citizens, then it amounts to the infringement of the sovereignty of their rights.

“The main issues which arise with related to the jurisdiction in a state over a transnational cyber fraud are the following

(a) Substantive Jurisdiction, where the act usually occur only partly if at all within the national territory and

(b) Investigative Jurisdiction, where they can conduct investigation and inquiries in foreign land. To proceed with these investigations there require adequate domestic as well as international law prescribing extra-territorial jurisdiction over cyber fraud. It also requires international cooperation and coordination among the countries through

---

<sup>397</sup> <http://docs.manupatra.in/newsline/articles/Upload/4730150C-4A12-4EBA-8CAF-F1146FDD5657.pdf>

<sup>398</sup>Investigating Cybercrime (2017), URL: [https://www.researchgate.net/publication/313164048\\_Investigating\\_Cybercrime](https://www.researchgate.net/publication/313164048_Investigating_Cybercrime) (visited on 14/1/2020) also see <https://cliffordodhiambo.wordpress.com>

numerous multilateral treaties or bilateral treaties, international convention and mutual legal assistance agreements.”<sup>399</sup>

However, cyber jurisdiction issues are covered in the Council of Europe’s Cyber Crime Convention, 2001 where it has provided that extra territorial jurisdiction of a country does not involve the ability of a state to enforce the jurisdiction. The Budapest Convention is the noteworthy convention and it has become the gold standard for drafting cyber law to other countries.<sup>400</sup> Budapest Convention provides power to police to access the server of other countries without any permission of the authority in order to access the electronic evidence fast as possible.<sup>401</sup> The main problem in cyber crime is that sometimes one country may not recognize relevant acts as an offence within their country. The Convention has played a significant role in addressing cyber issues and has shown the importance of cooperation amongst the international level to combat cyber criminals. Cyber jurisdiction remains important for the world, the Budapest Convention is applicable within the European States and it has shown urgent needs for the adoption of international instruments. In **“MacDonough v. Fallon MacElligott Inc.”**,<sup>402</sup> the court held that accessibility of commercial website's by residents standing alone, is not sufficient proof of personal jurisdiction over the creator of the site. The defendant having a website accessed by Californians is not sufficient enough to establish jurisdiction. Thus, the court further held that availability of the defendant's website to residents of California was

---

<sup>399</sup>Verma Sandhya, “The Challenges of Cyber War A Critical Evaluation” (2017) URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/277965/10/10%20\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/277965/10/10%20_chapter%204.pdf) (visited on 13.2.2020)

<sup>400</sup> Rattan Jyoti, Cyber Jurisdiction: A Seamy Side of Cyber Sovereignty With Special Reference To India (2018) 5 GNLU L. Rev. 52 URL: <https://www.scconline.com/Members/NoteView.aspx?enc=SIRYVC05MDAwMDY0NjcyJiYmJiY0M CYmJiYmU2VhcmNoJiYmJiZmdWxsc2NyZWVuJiYmJiZ0cnVlJiYmJiZjeWJlciBqdXJpc2RpY3Rpb 24mJiYmJkFsbFdvcmRzJiYmJiZnU2VhcmNoJiYmJiZmYWxzZQ==> (visited on 5.8.2019)

<sup>401</sup><https://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty>  
<sup>402</sup>1996 U.S. Dist. Lexis 15139 (S. D. Cal. August 5, 1996)

insufficient to create personal jurisdiction. Thus, the defendant website used by people outside their territorial boundaries cannot establish jurisdiction.”<sup>403</sup> Similarly, in “**Zippo Mfg. CO. v. Zippo Dot Com Inc.**,”<sup>404</sup> the court held that it is insufficient ground for exercising jurisdiction just by making information available on the internet for the user, as the website can be accessed from anywhere in the world.”<sup>405</sup>

Jurisdiction is the lawful ability of a government to subject a person to the Government legal processes. Jurisdiction is one of the biggest challenges to law enforcement in the information age. The territorial boundaries of a state create more problems with investigating officials since they have to examine the cybercrime within their local limits under local laws, which makes it limited jurisdiction for investigating processes. While cybercrime itself is a broader, less crime having cross-border issues, it makes it kind of compulsory to collect the evidence or investigate the foreign individual. To overcome this hurdle, the State has to develop a mechanism to collect evidence on the foreign territory without infringement on their territorial sovereignty of the state through the mechanism of mutual assistance.

### **3.7.1. Mutual Legal Assistance:**

“Mutual Legal Assistance (MLA) is the formal procedure by which the state can request and obtain evidence on foreign territory.” Through MLA, the state can obtain collected evidence upon request by law enforcement authorities. The Budapest Convention is the most important multilateral treaty in the cross- border cybercrime investigation. The Convention is essential as it focuses on the “harmonization of substantive criminal law through mutual

---

<sup>403</sup>MacDonough v. Fallon McElligott, Inc. URL: [http://www.internetlibrary.com/cases/lib\\_case177.cfm](http://www.internetlibrary.com/cases/lib_case177.cfm)

<sup>404</sup>952 F. Supp. 1119 (W. D. Pa. 1997)

<sup>405</sup> <https://cyber.harvard.edu/property00/jurisdiction/zipposum.html>



legal assistance where the state can similarly criminalize it. The Convention on Cybercrime obliges member states to create a contact point to ensure immediate mutual legal assistance twenty four hours a day.”<sup>406</sup> “This helps to create a system of international cooperation to eradicate cybercrime. The Convention imposes an obligation upon the parties in order to provide mutual assistance for the investigation proceedings for the collection of digital evidence by sharing the evidence through the authorities. The convention allows parties to appoint the designated official/ authority for the purpose of sending and answering all the assistance requested by the parties. In case of sensitive cases the request for the assistance of sharing evidence can be kept secret or confidential by requesting the parties to keep it secret because of the serious nature of the case. The Convention has specifically clarified that parties can request Mutual assistance in order to make search and seizure computer data within its territory, allow to have specified communication in order to collect or record the data required for digital evidence which need to be present before the courtroom.”<sup>407</sup>

Mutual Legal Assistance is a mechanism whereby countries cooperate with one another in order to provide and obtain formal assistance in order to ensure prevention, suppression, investigation and prosecution of crime to ensure that the criminal does not escape the due process of law for want of evidence available in different countries. India provides mutual legal assistance in criminal matters through Bilateral Treaties/Agreement, Multilateral

---

<sup>406</sup> Convention on Cyber-crime

<sup>407</sup>International Cooperation in Cybercrime: The Budapest Convention URL: <https://cis-india.org/internet-governance/blog/vipul-kharbanda-april-29-2019-international-cooperation-in-cybercrime-the-budapest-convention> (visited on 25.5.2020)

Tries/Agreements or International Convention. MLA requests are made by the Central Authority of India to the Central Authority of another country on the request of the investigating officer or investigating agency. The request can only be made to those countries with which India has bilateral treaty, multilateral treaty or international convention. Request for issue of a Letter of Rogatory shall be brought before competent court by the investigating agency with the prior permission of the Ministry of Home Affairs (MHA) and Government of India. India to enter into Mutual Legal Assistance Treaties with 42 countries by November 2019.

### **3.7.2. Uniform Cyber fraud Law**

“There is an absence of uniform cyber law at the international level to combat cyber fraud. Cyber fraud is a global phenomenon, in order to initiate the fight”<sup>408</sup> against cyber fraud needs to come from the same level. There should be uniform cyber law which can cover all the digital crime which occurs in cyberspace.”<sup>409</sup> “Cyber frauds being a global problem, the majority of countries have their own national laws that are covering cyber crime. Cyber fraud is creating difficulties for everyone in order to combat this crime. The country must form strengthened law because a person can be prosecuted for cyber fraud without the cyber fraud law unless it is considered as an illegal activity punishable by act of law. Harmonization of procedural provisions in global level amongst the countries would help in collecting evidence at global level by sharing information through international cooperation via treaties of ‘Mutual Legal Agreement’. With uniform cyber law we would have standard

---

<sup>408</sup>Cyber crime (slideshare.net)

<sup>409</sup>Pati Parthasarathi, Cyber Crime URL: [https://www.naavi.org/pati/pati\\_cybercrimes\\_dec03.htm](https://www.naavi.org/pati/pati_cybercrimes_dec03.htm) (visited on 24.5.2020)

procedural law for the investigation or production of digital evidence and harmonization of this law would ensure the digital evidence prosecuted is admissible in another country.”<sup>410</sup>

---

<sup>410</sup>International Cooperation in Cybercrime: The Budapest Convention URL: <https://cis-india.org/internet-governance/blog/vipul-kharbanda-april-29-2019-international-cooperation-in-cybercrime-the-budapest-convention> (visited on 25.5.2020)

## CHAPTER FOUR

### ROLE OF RBI

#### 4.1. Introduction:

The central bank of India RBI controls all the monetary policy of the country. According to the section 3 of the Act, “Reserve Bank of India has been constituted for the purpose of controlling over the management of the currency and further carrying on the business of banking having a common seal.”<sup>411</sup> As per provisions of Reserve Bank of India Act, 1934 RBI was established on the 1<sup>st</sup> April 1935.<sup>412</sup> This monetary institution was established during the British period in India. It plays an important role in maintaining and controlling different banks all over India. “In order to respond to economic trouble the central bank was founded in 1935.”<sup>413</sup> “During most of the pre-independence period, RBI was a private bank, though formed under a statute and its functions during that phase were confined to traditional central banking, i.e. note issue authority and banker to the Government. The initial phase of RBI was marked by several war and post-war developments including separation of Burma in 1937, the partition of the country in 1947, and nationalization of the RBI in 1949 which altered the area of operations of the RBI.”<sup>414</sup> “The Central Bank was set up for the purpose of providing finance to meet the expenses in war as well as to manage the debt so they have their own unique function and objectives. This Central Bank was founded as a

---

<sup>411</sup> Section 3 of RBI Act, 1934: Establishment and incorporation of Reserve Bank.

<sup>412</sup> Reserve Bank of India Act, 1934

<sup>413</sup> [https://shodhganga.inflibnet.ac.in/bitstream/10603/15993/8/08\\_chapter1.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/15993/8/08_chapter1.pdf) (visited on 4/06/2019)

<sup>414</sup> History of Reserve Bank of India - GKToday also see URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08_chapter%204.pdf) (visited on 31/03/2020)

special bank and it evolves into public sector institutions much later.”<sup>415</sup> “There is a different effort made for the establishment of the Reserve Bank of India. Warren Hasting, Governor of Bengal, reminded them of the need for a Central Bank in India in 1773.”<sup>416</sup> “The Reserve Bank of India was set up on the recommendation of the Hilton Young Commission.”<sup>417</sup> “British Government set up the Hilton Young Commission on Indian Currency and Finance in 1920.”<sup>418</sup> Thus, in 1926 Hilton Young Commission recommended setting up an institution that can be entrusted with the pure central bank functions<sup>419</sup> and it recommended the government for creating a separate central bank. The bill to give effect to the separate central bank was introduced in legislative banking but it was withdrawn due to the lack of certain agreement among the few sections of the people. “In 1931 The Indian Central Banking Enquiry Committee received the opinion for a separate central bank. RBI started its operations from April 1, 1935.”<sup>420</sup> “Since then, the role and functions of Reserve Bank have evolved through it all starting with private banks; the Reserve Bank was nationalized in 1949.”<sup>421</sup> Previously, the central office of Reserve Bank was established in Kolkata, Bengal, and later on, in 1937 it was permanently shifted to Mumbai.

---

<sup>415</sup>Reserve Bank of India Functions & Working Impacting Every Sector of The Economy & Touching Every Life Published by Dr. Rabi N Mishra, Chief General Manager and Principal, Reserve Bank Staff College, Chennai: November 2017 URL: [https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018\\_FCD40172EE58946BAA647A765DC942BD5.PDF](https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018_FCD40172EE58946BAA647A765DC942BD5.PDF)

<sup>416</sup>Chand Smriti, “Reserve Bank of India: Origin and Development”, URL: <http://www.yourarticlelibrary.com/banking/reserve-bank/reserve-bank-of-india-origin-and-development/26356>(visited on 20/8/2019)

<sup>417</sup> [https://shodhganga.inflibnet.ac.in/bitstream/10603/100409/4/04\\_chapter%201.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/100409/4/04_chapter%201.pdf) (visited on 5/06/2019)

<sup>418</sup><https://www.gktoday.in/gk/history-of-reserve-bank-of-india/>

<sup>419</sup> <https://rbidocs.rbi.org.in/rdocs/content/PDFs/89634.pdf> (visited on 5/06/2019)

<sup>420</sup>ibid

<sup>421</sup>[rbidocs.rbi.org.in](https://rbidocs.rbi.org.in)

Since the last 75 years, the “core function of reserve banks is to formulate and implement monetary policies with the objective of maintaining financial stability and ensuring its flows in the economy within our country.”<sup>422</sup> “The Reserve Bank of India has been designed in such a way to formulate the as directed by the policies of law enforcement agencies and to protect the customer interest as well as to maintain banking institutions.”<sup>423</sup> “The Reserve Bank is directed under Reserve Bank of India Act, 1934, they can issue different guidelines for maintaining the stability and maintaining the credits of India.<sup>424</sup> The primary role as suggested by the Act is the monetary stability as well as inclusive growth and development of the financial markets and institutions. Along with it, the preamble has also mentioned that in order to meet the challenges of the increasing economy and to maintain price stability, it is a requirement to have a modern monetary policy framework.”<sup>425</sup> The function of the reserve bank changed amid time as the nature of the Indian economy and banking institution changed.

The traditional functions of RBI as laid down by the statute were: (a) issues of currency; (b) banker to the government; (c) credit control measures; (d) the lender of last resort; (e) exchange control; (f) clearinghouse, etc.<sup>426</sup> The Reserve Bank of India even maintains the banking account to the government of India. RBI being the Central bank for all other banks, they issue the license to open branches as per the Banking Regulation Act 1949 and also control other banks.

---

<sup>422</sup>Reserve Bank of India: Functions and Workings URL: <https://rbidocs.rbi.org.in/rdocs/Content/PDFs/FUNCWWE080910.pdf> (visited on 2/8/19)

<sup>423</sup> *Supra* note 422

<sup>424</sup>The Preamble of the Reserve Bank of India Act, 1934

<sup>425</sup> Reserve Bank of India Act, 1934 URL: [rbidocs.rbi.org.in](https://rbidocs.rbi.org.in)

<sup>426</sup>Traditional Functions of Reserve Bank of India URL: <https://accountlearning.com/traditional-functions-of-reserve-bank-of-india/> (visited on 6/08/2019)

The structure of the banking system is determined by two basic factors i.e., economic and legal. The development of the economy and the spread of banking habits allows for increasing banking services in a country. Regulations for the formation of new banks are framed to meet specific needs and it affects the structure of banking as a whole.<sup>427</sup> “All banks are regulated by the RBI, so it issues from time to time different policies as needed for the banks smoothly.”<sup>428</sup>

## **4.2. RBI in Traditional Banking**

A bank is an organization which collects the deposits and advancing loans to the customers. Section 5(b) of Banking Regulation Act, 1949 is pertinent to mention according to the section banking as “accepting, for the purpose of lending or investment of deposits of money from the public, repayable on demand or otherwise, and withdrawals by cheque, draft, order or otherwise.”<sup>429</sup> “In Indian banking system the RBI is the apex body for dealing all matters relating to the banking system since it is the Central Bank of our country.”<sup>430</sup> Traditional functions are those which every central bank of the nation has to perform. These functions are the prime objectives with which banks are set up. In traditional banking, customers have to visit the branch personally during the working hours of banks. It consumes lots of time along with cost expenses. There are many traditional functions such as:

---

<sup>427</sup> [http://www.pondiuni.edu.in/storage/dde/downloads/finiii\\_ifs.pdf](http://www.pondiuni.edu.in/storage/dde/downloads/finiii_ifs.pdf) (visited on 4/08/2019)

<sup>428</sup>“The Indian Banking Sector: Recent Developments, Growth and Prospects” January 2013 URL: <https://www.ibef.org/download/Banking-Sector-04jan.pdf> (visited on 4/08/2019)

<sup>429</sup>Section 5(b) of Banking Regulation Act, 1949 <http://www.legalserviceindia.com/legal/article-3322-e-banking-frauds-and-indian-legal-prospective.html>

<sup>430</sup>“A Comparative Analysis of Customer Satisfaction in Nationalised and Private Banks in Madhya Pradesh 2001-2010” URL: <https://shodhganga.inflibnet.ac.in/bitstream/10603/114179/3/chapter-3.pdf> (visited on 4/8/2019)

i) **Issue of Currency Notes:**

Management of currency is a core central banking function and the RBI has the sole authority<sup>431</sup> or monopoly to issuing currency notes except one rupee note and coins of smaller denomination. The RBI has powers not only to issue and withdraw the currency but it can even exchange currency notes for other denominations. It issues these notes against the security of gold bullion, foreign securities, rupee coins, exchange bills, and promissory notes, and government of India bonds.

ii) **Banker to the Governments:**

The Imperial Bank of India performed as a banker to the Government before the formation of Reserve Bank of India. With the establishment of RBI, Imperial Bank ceased to be the banker to the Government and became a sole agent of the RBI. “As a banker to the Central Government and the State Government, the RBI provided many banking services such as acceptance of money on government account payment or withdrawal of funds and collection and transfer of funds through different ways.”<sup>432</sup> RBI shall transact Government business and they must accept money from the Central Government to make the payment in the credit account and carry on

---

<sup>431</sup> Section 22 of Reserve Bank of India Act, 1949: Right to issue bank notes- (1)The Bank shall have the sole right to issue bank notes in [India], and may, for a period which shall be fixed by the [Central Government] on the recommendation of the Central Board, issue currency notes of the Government of India supplied to it by the [Central Government], and the provisions of this Act applicable to bank notes shall, unless a contrary intention appears, apply to all currency notes of the Government of India issued either by the [Central Government] or by the bank in like manner as if such currency notes were bank notes, and references in this Act to bank notes shall be construed accordingly.

<sup>432</sup>Analysis Of Financial System Of RBI URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08_chapter%204.pdf) (visited on 5/8/2019)



other banking operations.<sup>433</sup> As per Section 21 of the RBI Act, the Bank has the right to transact Government business in centre<sup>434</sup> as well as in the State after making an agreement with any government for banking transactions and the management of the public debt and the issue of any new loans.<sup>435</sup> One of major role the Reserve Bank plays are the role of a banker to the government and thus perform the task of receiving and paying money on behalf of the several government departments.

iii) **Banker to the Banks:**

It acts as a central bank for other banks. Reserve Bank is the sole authority for running banks in India in order to regulate flow of currency.”<sup>436</sup> RBI is the bank of all banks in India as it provides the loan to banks/bankers and accepts deposits of banks.

iv) **Lender of last resort:**

The banks can borrow at the time of crisis from the Reserve Bank by keeping eligible securities as collateral.

---

<sup>433</sup>Section 20 of RBI Act, 1934: Obligation of the bank to transact Government business- The Bank shall undertake to accept monies for account of the Central Government and to make payments up to the amount standing to the credit of [its account], and to vary out [its exchange], remittance and other banking operations, including the management of the public debt [of the Union].

<sup>434</sup>Section 21 of RBI Act, 1934:(1)The [Central Government] shall entrust the Bank, on such conditions as may be agreed upon, with all [its] money, remittance, exchange and banking transactions in India, and, in particular, shall deposit free of interest all [its] cash balances with the Bank. Provided that nothing in this sub-section shall prevent the Central government from carrying on money transactions at places where the Bank has no branches or agencies, and the Central Government may hold at such places such balances as it may require. (2) The Central Government shall entrust the Bank, on such conditions as may be agreed upon, with the management of the public debt and with the issue of any new loans. (3) In the event of any failure to reach agreement on the conditions referred to in this section the Central Government shall decide what the conditions shall be.

<sup>435</sup> Section 21A of RBI Act 1934: Bank to transact Government business of States on agreement.

<sup>436</sup>Emerging Role as a Bankers’ Bank URL: at <https://rbidocs.rbi.org.in/rdocs/content/PDFs/89639.pdf> (visited on 3/3/2019)

### 4.3. RBI in Electronic Banking

“The advanced economy banks reorient their banking business, makeshift from traditional banking to internet banking or e-banking. The growing hi-tech companies have emerged, providing banking services using digital innovations through online platforms.<sup>437</sup> Reserve Bank monitors and reviews the legal requirements for internet banking so that they can ensure the challenges may not pose any kind of threat with regards to internet banking. Reserve Bank of India has laid down in detail the policy guidelines, and procedures to follow for detection, investigation, taking integral action; as well as, prevention and reporting of various types of bank frauds. It is a well-known fact that in a large majority of fraud cases, banks do not follow the guidelines prescribed by the central bank. The central bank takes various steps to control fraud in banks.<sup>438</sup>

“The banks themselves have an onus of preventing Frauds, whereas RBI has an advisory role to play. RBI has frequently circulated directions and guidelines to the banks for necessary safeguard and preventive measures against incidences of frauds. Due to an increase in cyber frauds incident, RBI had advised all banks to introduced security standard mechanism up to certain minimum checks and balances like introduction of certain secure payment modes by certain factors such as transactions done without the presence of a card and setting certain limits of the cash for

---

<sup>437</sup> “Committee on the Global Financial System: CGFS Papers No 60 Structural changes in banking after the crisis”, January 2018 URL: <https://www.bis.org/publ/cgfs60.pdf> (visited on 3/3/2019)

<sup>438</sup> Dr. Madan Lal Bhasin, “*An Empirical Study of Frauds in the Banks*”, Vol. 4, No. 07, October 2015 European Journal of Business and Social Sciences

withdrawal for their safety against cyber fraud.<sup>439</sup> The system of banking also places a threshold limit on international usage of debit/credit cards. There is also a provision of reviewing constantly, the pattern of card transactions. This should be done in coordination with customers. An updated through text messages about the accounts is next step.<sup>440</sup> Securing monetary stability in India and modernizing the policy framework to meet economic challenges. “Reserve Bank of India has defined fraud through similar offences as provided in Indian Penal Code 1860.<sup>441</sup>

While internet banking has improved its efficiency and convenience, it has also posed several challenges to the regulators and supervisors. The Reserve Bank of India have played a very important role in the digital development in India and thus introduced many new initiative of maximization of use of internet, time and again. As a regulator and supervisor, the Reserve Bank of India (RBI) has made substantial improvement in consolidating the existing payment and settlement systems, and in advancement technology with a view of establishing an efficient, integrated and secure system functioning in a real-time environment, which has further helped the development of internet banking in India.<sup>442</sup> The RBI has been preparing to upgrade itself as a regulator and supervisor of the technologically dominated financial system. It has issued guidelines on risks and control on computer and telecommunication systems to

---

<sup>439</sup> Two factor authentication in case of “card not present” transaction, converting all strip based cards to chip based cards for better security, issuing debit and credit cards only for domestic usage unless sought specifically by the customer. See: Bank Frauds in India- An Analysis, URL: <https://www.bankingfinance.in/bank-frauds-in-india-ananalysis.html>

<sup>440</sup>Varun Tripathi, *Frauds and Cyber Frauds in Banking Sector* (2014) PL December 76 also see [https://www.rbi.org.in/scripts/BS\\_SpeechesView.aspx?Id=826](https://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826)

<sup>441</sup>The includes offences mentioned the Indian Penal Code- Criminal misappropriation; criminal breach of trust; fraudulent encashment with the use of forged documents/instruments/forged accounts, manipulation of books of account, conversion of property, unauthorized credit facilities extended for reward or for illegal gratification, negligence, and cash shortages, cheating, and forgery, irregularities in foreign exchange transactions. RBI / 2005-06/190 DNBS (PD) C.C. No.59 /03.10.42/2005-06 [https://m.rbi.org.in/Scripts/BS\\_ViewMasCirculardetails.aspx?id=9808](https://m.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9808)

<sup>442</sup> Dr. Pooja Goel, “*Electronic Banking*”, University of Delhi URL: <https://sol.du.ac.in/mod/book/view.php?id=1225&chapterid=855> (visited on 5/3/2019)

all banks, advising them to evaluate the risks inherent in the systems and put in place adequate control mechanisms to address these risks.

In the early 1980s two committees were set for regulating banks in India.<sup>443</sup> They developed and implemented or installed two models of automation in the branch. The Rangarajan committee constituted in 1988 further drew up transactions through electronic payments.<sup>444</sup> In July 1999, Dr. Vasudevan Committee submitted a Report on technology Upgradation in the banking sector making recommendations for the legal implementation of Information Technology in banking. With the adoption of digitized banking system the Reserve Bank of India Act, 1934 needs for an amendment in a view to providing RBI with the new desired regulatory and supervisory powers for advanced payment and settlement systems. Further, in order to formulate electronic banking services a separate legislation on electronic funds transfer systems is needed.<sup>445</sup>

“The Reserve Bank of India has set up the Working Committee for setting up internet banking in different banks to examine different aspects of internet banking which focused mainly on, security issues, legal issues, and regulatory or supervisory issues.”<sup>446</sup> These notifications have been issued for all Scheduled Commercial Banks. As per the Reserve Bank of India, different departments for cyber frauds should be established and maintain security policies as required for security systems.”<sup>447</sup> Banks

---

<sup>443</sup>To draw up the first blueprint for computerization and mechanization in the banking industry a committee was formed under the chairmanship of Dr. C. Rangarajan.

<sup>444</sup>For computerization and automation in funds transfer, e-mail, BANKNET, SWIFT, ATMs, internet banking, etc also see: Dr. Tejinderpal Singh, “*Security and Privacy Issues in E-Banking: An Empirical Study of Customers’ Perception*”, October 2013 URL: [http://www.iibf.org.in/documents/research-report/Tejinder\\_Final%20.pdf](http://www.iibf.org.in/documents/research-report/Tejinder_Final%20.pdf) (visited on 4/3/2019)

<sup>445</sup>Bindra P. S, “IT Implementation in Banking- Legal Implications”, September 30, 1999 URL: <https://rbi.org.in/scripts/PublicationsView.aspx?id=1572> (visited on 2/3/2019)

<sup>446</sup>Internet Banking in India- Guidelines, RBI Vide Circular DBOD. COMP.BC.No.130/07.03.23/2000-01 Dated June 14, 2001

<sup>447</sup>[http://www.iibf.org.in/documents/research-report/Tejinder\\_Final%20.pdf](http://www.iibf.org.in/documents/research-report/Tejinder_Final%20.pdf)

are exposed to high technology risk because it always stays connected with the internet so for safety measures banks should use the proxy server type of firewall which restricts the direct connection within the bank and internet.<sup>448</sup> Public Key Infrastructure (PKI) is the widely accepted technology in banks for securing internet banking services.<sup>449</sup> It is important for banks to report all the suspicious moments regarding banking transactions and it needs to be considered while framing any policies for internet banking security. Banks should continuously keep on reviewing their security infrastructure and policies on a regular basis.

“Until the installation of PKI (public Key Infrastructure) there should be the usages of SSL (Secure Socket Layer) to ensure server authentication and for securing browser to web server communication they must use at least 128-bit.”<sup>450</sup> The Reserve Bank of India has provided a new circular for implementation of Internet Banking which “banks need to follow strictly for the procedures of opening deposit accounts to safeguard against unscrupulous persons opening fictitious accounts to use them as a conduit for a fraudulent transaction.”<sup>451</sup> The Reserve Bank of India is sole supervisor for the entire banks of India; it covers the entire risks associated with electronic banking and provides new guidelines or policies for electronic banking. It is the duty of every bank to follow guidelines issued by the Reserve Bank of India to develop a clear Customer Acceptance Policy laying down precise criteria for the acceptance of customers.<sup>452</sup> No banking company, financial institution, and intermediary shall allow the opening of or keeping any anonymous account or any account having fictitious

---

<sup>448</sup><https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0>

<sup>449</sup>In unavailability of PKI (Public Key Infrastructure) banks should use SSL (Secured Socket Layer) which authentication and use of client side certificates issued by the banks themselves and the use of at least 128-bit SSL for securing browser to web server communications and encryption of sensitive data like passwords. See: <https://www.altaro.com/hyper-v/public-key-infrastructure/>

<sup>450</sup> B. Dutta & R.P Shukla, Banking Laws (Principles, Practice & Procedure), Dwivedi Law Agency, Allahabad, Volume.1 Edition 2010

<sup>451</sup> RBI Vide Circular DBOD. No. GC. BC. 193/ 17.04.001 dated November 18, 1993

<sup>452</sup> RBI Vide Circular DBOD. AML. BC. No. 11/14.01.001/2012-13

names or accounts on behalf of other persons whose identity has not been disclosed or cannot be verified.<sup>453</sup> For the opening of the account online requests can also be accepted but there is an obligation on the part of banks to make an inquiry about the prospective customer. It is the duty of the bank to make verification of the identity of a customer and they must check all the required documentation before creating customer's accounts.<sup>454</sup>

Reserve Bank of India has provided guidance on classifying and reporting of fraud. RBI has gradually been increasing its focus on frauds committed on banks by borrowers and has over a period of time set up various mechanisms towards mitigating the risk. The new concept of 'Red Flagged Account (RFA)' has been introduced in the existing fraud risk management framework with loan frauds in relation to exposures in excess of INR 50 crore. A key requirement for the RFA is that it proactively identifies loan accounts with Early Warning Signal (EWS) or typical.<sup>455</sup>

In 2015, the Reserve Bank of India introduced new mechanisms for banks to check loan frauds by taking proactive steps by setting up a Central Fraud Registry, introduced the concept of Red Flagged Account and Indian Investigating Agencies. On 5<sup>th</sup> November 2015 RBI issued uniform guidelines on internet banking for Cooperative Banks. These guidelines are for all licensed cooperative banks including Urban Cooperative Banks (UCBs), State Cooperative Banks (StCBs), and District Cooperative Banks (DCBs). The guidelines are related to internet banking (view only) facility and internet banking with a transaction facility. The service offered under internet banking 'view only' facility, it requires two-factor authentication or One

---

<sup>453</sup> RBI Vide Circular DBOD. AML. BC. No. 113 /14 .01.001/2009-10

<sup>454</sup> RBI Vide Circular DBOD. COMP. BC. No. 130/ 07.03.23/ 2000-01 (Para 7.2.1) Reserve Bank of India - Notifications (rbi.org.in)

<sup>455</sup> Framework for loan fraud URL: <https://home.kpmg/content/dam/kpmg/pdf/2015/06/Framework-Loan-fraud.pdf>

Time Password (OTP) and the banks have to adopt the security features prescribed in the circular.<sup>456</sup> Similarly, on 1<sup>st</sup> July 2015, RBI issued a “Master Circular on Fraud-Classification and Reporting”<sup>457</sup> which enclosed all the instructions or guidelines about the classification of frauds or reporting of frauds to RBI, etc. Since the incidence of fraud is a matter of concern, therefore, its banks’ responsibilities to prevent fraud. From time to time “RBI being the central bank as a regulator of Indian banks has been advising other banks about the major fraud-prone areas and their necessary safeguard for the prevention of fraud.”<sup>458</sup> In a different circular issued by RBI, it has been circulating to banks all the details of fraud earlier so that inappropriate procedures can introduce a necessary safeguard.

Banks are allowed to frame their own policy for investigation of Cyber fraud which needs to be followed in an effective way with the prior approval of the Reserve Bank of India. Fraud can be classified as per the Indian Penal Code, 1860.<sup>459</sup> The Reserve Bank of India has set a Central Payment Fraud Registry to track frauds in the payment system. All banks report banking fraud to the central fraud monitoring cell of the Reserve Bank. On 1st July 2016, RBI forwarded the Master Circular on “Fraud-Classification, and Reporting’. The Master Circular is applied to scheduled commercial banks and FIs operating in India. They provide directions for providing a

---

<sup>456</sup>RBI Notification dated November 05, 2015 URL: <https://rbi.org.in/Scripts/NotificationUser.aspx?Id=10111&Mode=0>

<sup>457</sup>RBI Master Circular :RBI/2015-16/1 dated: July 1, 2015 URL: [https://m.rbi.org.in/Scripts/BS\\_ViewMasCirculardetails.aspx?id=9808](https://m.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9808)

<sup>458</sup> ibid

<sup>459</sup>Classifications of frauds are basically done as per the provisions of Indian Penal Code (IPC), as under:-

- a. Misappropriation and criminal breach of trust.
- b. Fraudulent encashment through forged instruments, manipulation of books of account, or through fictitious accounts and conversion of property.
- c. Unauthorized credit facilities extended for reward or for illegal gratification.
- d. Negligence and cash shortages.
- e. Cheating and forgery.
- f. Irregularities in foreign exchange transactions.
- g. Any other type of fraud not coming under the specific heads as above

framework to the banks enabling them to detect and report fraud early as possible and they must take action for the fraud by reporting to the appropriate investigating agencies.<sup>460</sup> They set up a fraud monitoring cell and have instructed all banks about risk management. The fraud monitoring, is controlled by the bank authorities together with the fraud investigation<sup>461</sup> particularly fraud involving bigger amount. The RBI has asked banks to disclose fraud cases and make provisions for them not exceeding four quarters from the date during which it has been detected. Banks as per the notification must scrupulously adhere to the provided guidelines by RBI on classification and reporting of the frauds.”<sup>462</sup> Therefore, Reserve Bank of India should frame guidelines for fraud reporting to bank authorities and liable in case of compliance with the rules as prescribed under Banking Regulation Act, 1949.<sup>463</sup> “RBI

---

<sup>460</sup>It also enables faster circulation of information by the Reserve Bank of India to other banks regarding the details of frauds, unscrupulous borrowers and related parties, based on banks’ reporting so that necessary safeguards or preventive measures, procedures and internal checks should be introduced and caution exercised while dealing with such parties by banks.

<sup>461</sup>Bank’s CEO, Audit Committee of the Board, and the Special Committee of the Board

<sup>462</sup>RBI Notification dated July 01, 2016 URL: <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD28A4C421E7F7724C07B38E3C6207F3548E.PDF>

<sup>463</sup>Section 47A of Banking Regulation Act: Power of Reserve Bank to impose penalty-

(1) Notwithstanding anything contained in section 46, if a contravention or default of the nature referred to in 1[sub-section (2) or sub-section (3) or sub section (4)] of section 46, as the case may be, is made by a banking company, then, the Reserve Bank may impose on such banking company[(a) where the contravention or default is of the nature referred to in subsection (2) of section 46, a penalty not exceeding twenty lakh rupees in respect of each offence and if the contravention or default persists, a further penalty not exceeding fifty thousand rupees for everyday, after the first day, during which the contravention or default continues; (b) where the contravention is of the nature referred to in subsection (3) of section 46, a penalty not exceeding twice the amount of the deposits in respect of which such contravention was made; (c) where the contravention or default is of the nature referred to in subsection (4) of section 46, a penalty not exceeding one crore rupees or twice the amount involved in such contravention or default where such amount is quantifiable, whichever is more, and where such contravention or default is a continuing one, a further penalty which may extend to one lakh rupees for everyday, after the first day, during which the contravention or default continues.]

[(2) For the purpose of adjudging the penalty under sub-section (1),the Reserve Bank shall serve notice on the banking company requiring it to show cause why the amount specified in the notice should not be imposed and a reasonable opportunity of being heard shall also be given to such banking company.]

[4(3) xxx ]

(4) No complaint shall be filed against any banking company in any court of law in respect of any contravention or default in respect of which any penalty has been imposed by the Reserve Bank under this section.

(5) Any penalty imposed by the Reserve Bank under this section shall be payable within a period of fourteen days from the date on which notice issued by the Reserve Bank demanding payment of the sum is served on the banking company and in the event of failure of the banking company to pay the sum within such period, may be levied on a direction made by the principal civil court having



has divided electronic banking into two categories i.e. Remote/online payment transactions (a transaction that does not require a physical payment instrument e.g. internet banking, mobile banking) and another one is face-to-face/proximity transaction (a transaction which requires physical payment instrument). In order to have successful secure electronic payment bank required to frame policy for security system considering KYC of their banks.<sup>464</sup> There must be an advanced robust and dynamic fraud detection and prevention mechanism in banks. The customers must mandatorily register their phone number in banks for SMS alerts and register their email, for electronic banking transactions details. Upon receipt of unauthorized electronic transaction information from the customer, the banking authority must take immediate action by blocking the account and follow other procedure.”<sup>465</sup>

Banking transactions in the present days have become more web-based using internet banking, credit card, or debit card. Banks even after spending more than three times on their financial security system had not been able to abort the hackers from committing frauds. Hackers using advanced notorious technology are committing banking frauds or unauthorized transactions. In 2017, Reserve Bank of India (RBI) drafted “a regulation<sup>466</sup> where it has clearly laid down certain criteria to which extend

---

jurisdiction in the area where the registered office of the banking company is situated; or, in the case of a banking company incorporated outside India, where its principal place of business in India is situated: PROVIDED that no such direction shall be made except on an application made to the court by the Reserve Bank or any officer authorised by that Bank in this behalf

(6) The court which makes a direction under sub-section(5) shall issue a certificate specifying the sum payable by the banking company and every such certificate shall be enforceable in the same manner as if it were a decree made by the court in a civil suit.

(7) Where any complaint has been filed against any banking company in any court in respect of the contravention or default of the nature referred to in subsection (3) or, as the case may be, sub-section (4) of section 46, then, no proceedings for the imposition of any penalty on the banking company shall be taken under this section.

<sup>464</sup><https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11040>

<sup>465</sup>RBI Notification on “Customer Protection- Limiting Liability of Customers of Co- operative Banks in Unauthorized Electronic Banking Transaction”, dated 14<sup>th</sup> December 2017 Reserve Bank of India - Index To RBI Circulars

<sup>466</sup>News Special 18 dated 24<sup>th</sup> July 2017 URL: <https://www.news18.com/news/india/banking-frauds-who-is-responsible-bank-or-you-1471503.html>

customers will be held liable for the unauthorized electronic transaction or fraud committed. The electronic transaction has categorized into two: (i) electronic payment without any physical presence and (ii) face-to-face/proximity transactions it needs instrument for payments at the time of the transaction through credit or debit card (i.e. presence of debit or credit card for ATM transactions). As per the regulation, the extent of customer liability is determined on the basis of negligence of the customer or third party breach towards the banking system.”<sup>467</sup> “If such a transaction has occurred due to the customer’s carelessness or negligence by disclosing the card details or passwords to some other person than for such transaction, the entire loss liability will be on part of the customer. And customers will have to bear the liability for the loss. The customer on the other side will have absolutely no liability if the unauthorized transaction has occurred due to the carelessness of bank staff. In the case of third party breach when unauthorized transaction fraud has been carried out by a third party in such situations the inadequacy lies with none of the two i.e. bank/customers. In such a case, liability of the customer depends on the date of informing the bank authorities”<sup>468</sup> or reporting within three days of unauthorized transaction<sup>469</sup> liability will be zero. And the reporting within seven days will be on the basis of bank policies.<sup>470</sup>

RBI on 19<sup>th</sup> October 2018 provided the framework for basic cybersecurity primary and cooperative banks. It stated that the number, frequency, and impact of cyber attacks or incidents have increased in the financial sector including banks. There is an

---

<sup>467</sup> <https://www.news18.com/news/india/banking-frauds-who-is-responsible-bank-or-you-1471503.html>

<sup>468</sup> Online banking frauds: RBI says no loss to customer if fraudulent transaction reported in 3 days dated July 07, 2017 URL: <https://www.firstpost.com/business/online-banking-frauds-rbi-says-no-loss-to-customer-if-fraudulent-transaction-reported-in-3-days-3783491.html>

<sup>469</sup> Receipt of communication implies the date on which individuals receive SMS, email or the bank explanation regarding the unauthorized transaction.

<sup>470</sup> <https://www.news18.com/news/india/banking-frauds-who-is-responsible-bank-oryou-1471503.html>

urgent need to install a robust cybersecurity framework to ensure adequate security of their assets; therefore it becomes essential to enhance the security of the urban cooperative banks from cyber threats by improving the current defences in addressing cyber risks.<sup>471</sup> With the emerging threat of cyber fraud, the Department of Information and Technology is working for continuous protection against the cybersecurity threat. The RBI report said they are taking effective steps to further enhance the levels of protection against cyber risk. It further said that to strengthen the cybersecurity in Indian banks they had focused on theme-based IT examination during 2018-2019 and the increasing popularity of digital payments, data protection, and cybersecurity norms were strengthened and Know Your Customer(KYC) norms were modulated further to make them more effective.<sup>472</sup> “The volume of cyber fraud at banks has doubled every year. According to a report by RBI, a total of 2,059 cases of cyber fraud were reported in 2017-18 amounting to Rs. 109.6/- crore whereas in 2016-2017 cyber fraud cases was 1,372 amounting to Rs. 42.3 crore.”<sup>473</sup> With the rise of the impact of cyber attacks in banks, the Reserve Bank of India circular to banks urges them to take adequate measures to tackle cyber criminals. Banks were asked to make continuous surveillance by testing for vulnerabilities through a Security Operations Centre (SOC) that is constantly updating on the nature of emerging cyber threats.<sup>474</sup>

The Reserve Bank of India has issued a revised direction for banks regarding financial inclusion, customer protection and fair practices in banking operation by providing

---

<sup>471</sup> RBI Vide Circular DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19

<sup>472</sup> The Economic Times dated: 3<sup>rd</sup> September 2018

<sup>473</sup>The Economic Times dated: 2<sup>nd</sup> January 2019 URL: <https://economictimes.indiatimes.com/industry/banking/finance/banking/watch-out-cyber-fraud-cases-in-banks-are-spiking/articleshow/6734975>

<sup>474</sup> RBI circular June 2016

separate guidelines.<sup>475</sup> There is an increase in digitalization in both the banks; likewise there is an increase of usage of digital payment. Different applications for the online payment system have been developed and there is an increase in grievances/complaints from the customers regarding incidents of online fraud. After considering the customer grievances related to unauthorized electronic banking transaction, Reserve Bank of India issued the revised guidelines for determining the liability of customers for unauthorized electronic banking transactions.<sup>476</sup>

In order to carry out safe electronic banking transactions the bank has designed advanced technology having appropriate systems and procedures to ensure safety as well as security of customers by making it mandatory to register SMS alerts or email alerts so that they can send their transaction details to customers. Banks for security measures provide customers with One Time Passwords (OTP) to their registered phone number/emails as a gateway for confirmation or authentication from the account holder. As per the guideline provided by RBI for reporting of unauthorized electronic banking transactions they must notify the bank regarding unauthorized electronic transactions at earliest as possible otherwise there is a high risk of further fraudulent transaction if the customer delay for informing the bank so it is a loss to both the bank and customers. In order to make immediate reporting by customer bank has provided 24 x 7 accesses through multiple channels such as bank website, toll-free helpline number, direct reporting at home branch, SMS, registering complaints, Interactive Voice Response (IVR). On receiving the complaint, the bank will immediately block the internet and mobile banking facilities of the customer accounts. Customers will be entitled to have zero liability in case the contributory fraud,

---

<sup>475</sup>Customer Protection for Limiting Liability of Customers in Unauthorized Electronic Banking Transaction (EBT) for the year 2018-2019 URL: [policy-for-customer-protection-for-limiting-liability-of-customers.pdf](https://www.canarabank.com/policy-for-customer-protection-for-limiting-liability-of-customers.pdf) (canarabank.com)

<sup>476</sup>[policy-for-customer-protection-for-limiting-liability-of-customers.pdf](https://www.canarabank.com/policy-for-customer-protection-for-limiting-liability-of-customers.pdf) (canarabank.com)

negligence or deficiency are done on the part of the Bank and if the unauthorized electronic transactions are made with negligence or deficiency by the bank. If there has been a third party breach where deficiency occurs due to technical inefficiency, inform it within three days after receiving a message about unauthorized electronic banking transaction then there will be zero liability of a customer.

“The customer will be liable for the entire loss, in case the loss or occurrence of unauthorized electronic transaction due to negligence of customer by sharing payments details, unless customer informs bank regarding fraudulent transaction and any loss occurring thereafter bank will take responsibility.”<sup>477</sup> “Unauthorized transactions are caused due to technical failure and inform the bank within seven days then liability will be limited but customers have to pay a partial amount of such transaction as mentioned in policies of RBI.”<sup>478</sup>

Fraudsters fraudulently send emails through their fake banking website providing loan offers or provide credit or debit cards and they will ask the account holder bank details by clicking on the link sent by them. Many people are not aware that the bank never sends such links asking their bank details or they never make any phone calls about account details or mention about expiring cards etc. “Reserve Bank has clarified that the bank never issues communication asking for bank account details for any purpose.”<sup>479</sup> It has come to the notice of RBI that a fraudulent email has been sent and signed in its name as ‘Reserve Bank of India’. The RBI clarifies that it has not sent any such mail and public receiving emails are asked to caution and not to open such

---

<sup>477</sup>RBI circular DCBR.BPD.(PCB/RCB). Cir.No.06/12.05.001/2017-18

<sup>478</sup> Maximum liability of a customer under paragraph 7 (ii) of RBI/2017-18/109 dated: 14, 2017 URL: [https://www.rbi.org.in/Scripts/BS\\_CircularIndexDisplay.aspx?Id=11188](https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11188)

<sup>479</sup> RBI Press Releases: Dated April 05, 2011

emails or attachments which may lead to fraudulent transactions.<sup>480</sup> The Reserve Bank of India has also issued notice to alert the public regarding credit card fraud where fraudsters issue credit cards in the name of the Reserve Bank. RBI tries to explain the modus operandi, how members are allowed to withdraw a certain amount of money and after gaining their confidence the fraudster will direct the victim to deposit money into the same bank account and soon after the deposition of money the card stopped working. It is important to keep in mind that the bank never asks or provides online credit card or account details. “Those offers can be made in the name of recognized public institutions which can be easily recognized and traced by the customers.<sup>481</sup> So public members need to be careful about such fake emails and if such things are going on then rather they should immediately lodge a complaint with the Cyber Crime branch of the Police or local police or Cyber Crime Authorities against fictitious offers of money even from abroad.<sup>482</sup>

With the passing of time, there are now numbers of a delivery channel that are provided by the bank for their banking services extension. Mobile banking is one of the delivery channels and with the rapid growth of users and wide networks coverage has made this channel important for extending banking service to the customers. “Banks have started new services for customer convenience that offer information-based services such as balance inquiry, transaction inquiry, to locate the nearest ATM/branch, etc.”<sup>483</sup> Banks should follow the security standards as provided by RBI such as banks are required to put risk mitigation measures like transaction limits for

---

<sup>480</sup>RBI Press Releases: Dated Sep14, 2012

<sup>481</sup>Such as banks, International Monetary Fund (IMF), Income Tax authorities or customs authorities, or public figures like Governor Dr. Raghuram Rajan or other senior RBI officials.”

RBI Press Releases Dated: Nov 21, 2014 URL: <https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/IEPR1046CR1114.PDF>

<sup>482</sup>ibid

<sup>483</sup>Mobile Banking transactions in India- Operative Guidelines for Banks URL: [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=1660](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1660)

online transfer per transaction, daily, weekly, transaction velocity limit, fraud checks, etc. “Banks providing mobile banking must complete and follow all the security measures provided by the RBI which are required for making secure and authentication of mobile banking transactions”<sup>484</sup> that are being set up by the Reserve Bank of India. Mobile banking authentication can be permitted only by the validation through a two-factor authentication and one of the factors of authentication shall be MPIN<sup>485</sup> (Mobile banking Personal Identification Number).

---

<sup>484</sup> Singh Tejinderpal, Security and Privacy Issues in E-Banking : An Empirical Study of Customers’ Perception Indian Institute of Banking and Finance (IIBF) October 2013 URL: [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=1660](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1660)

<sup>485</sup> MPIN is Mobile Banking Personal Identification Number. It works as a password when transaction is done using mobile and it is four digit (six digits in some bank) secret codes similar to the ATM pin.

## **CHAPTER FIVE**

### **JUDICIAL TRENDS IN INDIA AND EUROPEAN UNION**

The internet has made a shift in technology around the globe. India being a part of it has also felt a shift in information technology. The country has witnessed a vital transformation in the traditional banking system. Almost every activity is guided and regulated by the computers as the world is depending more on information technology. The technology has made a shift of traditional banking towards paperless banking with digital innovation where the services are more convenient and the transactions can be done through ATM, Credit/Debit Cards, Online Payment, etc. This shift of transformation of banking with a better technology facility is a boon in the country.

New technologies have always brought problems as well as solutions. The use of computer technology has not only helped governments and individuals but it has also enabled criminals with sophisticated computer knowledge to use computers in illegitimate ways. Cyber criminals got the opportunity to break laws and commit traditional crimes in non-traditional ways. It is difficult to determine when and where cyber fraud occurs.

Although internet banking is the most convenient and cheapest mode of service provided to the customers, due to lack of knowledge and unawareness among the public made them an easy target of cyber fraud. Cyber fraud is emerging as a new challenge for national as well as for our economic security. Many financial institutions, companies, public in general and much other private and public organization are at risk. Cyber fraud being of intangible nature it does not require any



kind of physical presence of the accused at the time of the fraud. Indian judiciary is playing an important role in dealing with cyber crimes with the Information Technology Act, 2000 and Amendment Act 2008. But the judiciary is inadequate to deal with cases of cyber fraud which has become a major challenge for them.

“The misuse of the technology has created the need for the robust enactment and implementations of stricter cyber laws. Today in the digitalized era computers play a major role in almost every crime that is being committed. Criminals complete their crime creating software to disrupt the system each improving or adapting with time as per their own needs but the question that requires most attention is whether this present cyber law is capable of controlling the growing cyber fraud activities.”<sup>486</sup>

“The Information Technology Act, 2000 clearly stipulates the cognizance of cases should be taken by the appropriate courts and must be governed by Criminal Procedure Code. In spite of the act much less numbers of cases have been filed and tried by the courts in India because of the number of factors like ignorance of filing cases, pendency after filing, jurisdictional conflicts, improper investigations on part of law enforcement agencies, lack of knowledge on part of law enforcement and interpretation agencies etc.”<sup>487</sup>

“The important function of the judiciary is to interpret the laws with the purpose to find out the real intention of the legislature and the court does not only legislate but also interprets the existing laws.”<sup>488</sup> The Court must achieve a balance between the

---

<sup>486</sup> R.M Kamble & C Vishwapriya, “Cyber Crime And Information Technology”, NALSAR Law Review Vol-4 2008-2009

<sup>487</sup>Dr. Jetling Yellosa, “Cyber Crimes and Legal Implications”, International Journal of Law, Vol. 2 Issue 2 (March 2016)

<sup>488</sup>Cyber Crime in India: Legislative And Judicial Response URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/12/12\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/12/12_chapter%204.pdf) (visited on 24/3/2020)

old and rigid laws on the one hand and the advanced technology on the other. The judiciary always acts with the need, demands of the changing scenario in a society. Traditional judicial system would be hard to meet litigation needs under the circumstances of development in advanced society with technology. In the case of the “**State of Punjab &Ors v M/S. Amritsar Beverages Ltd. &Ors**, Supreme Court observed:

Internet and other advanced information technologies being boon to our society brought with them those issues which were not foreseen by law, such as, for example, problems in determining statutory liabilities. Law enforcement was unaware about new crime evolving in society and with advancement technology they are facing challenges to handle these new eras of technology. Present situation demands for subjects experts in a profession to tackle new situations. There were various new developments in society leading to various new different kinds of crimes which remain unnoticed for our legislature and Information Technology Act, 2000 although was amended by amendment act of 2008 to include various kinds of cyber crimes and only the punishments for few different offences related to computer are included which are creating difficulties for authority dealing with such cases in future.”<sup>489</sup>

The first problem faced by criminal law systems is that existing criminal offences fail to cover the newly emerged forms of cyber wrongdoing. India saw its first cyber crime convection in 2003 in the **Sony Sambandh.com case**.<sup>490</sup> Fact of the case: - NRI

---

<sup>489</sup>State of Punjab & Ors v. M/S. Amritsar Beverages Ltd. &Ors decided on 8 August, 2006 URL: <https://indiankanoon.org/doc/283127/> (visited on 12/3/2020) also see <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>

<sup>490</sup> CBI vs. Arif Azim, 2003

enter website *www.sonysambandh.com* order Sony colour television set and a cordless headphone and asked to deliver the items at Noida to Arif Azim. Transactions for payments were made through credit cards. They deliver the same in said address. The credit card agency received a call one day and told us that there had been an unauthorized transaction from their card which they had not done.”<sup>491</sup>

The Central Bureau of Investigation (CBI) agency received a complaint of cyber fraud. They registered the case under Section 418, 419, and 420 of Indian Penal Code. In this case police arrested a call centre employee of Noida. This employee acquired the credit card details of an American. The detail he used in doing some unauthorized transaction later. The police filled a case against him under Section 418, 419 and 420 of the IPC and on investigated recovered some costlier items from his house.<sup>492</sup> The court held that “it is the first cybercrime in India. The accused was 24 years old and it is the first convicted case in India so they took decisions in a very lenient manner. Accused was released on probation of one year. In absence of cyber law Indian legislation can provide significant judgement that is not covered under the Information Technology Act 2000.”<sup>493</sup>

In **ICICI- Pune Bank Fraud case**<sup>494</sup> three people were held guilty for an online credit card scam. Ahmead Sikandar Shaikh was an employee at the branch of State Bank of India who along with two his other friend Sanjeet Mahavir Singh Lukkad and Dharmendra Bhika Kale misused the customer’s credit card details through the means of online booking of air-tickets. Cyber Crime Investigation (CBI) Cell caught these

---

<sup>491</sup> Singh Talwant, Cyber Law & Information Technology  
URL:<https://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>

<sup>492</sup><http://legalserviceindia.com/legal/article-3210-cyber-crime-a-hindrance-in-digitalworld>.

<sup>493</sup>ibid

<sup>494</sup>Cyber Crime Law and Practice URL:  
[https://www.icsi.edu/media/webmodules/publications/Cyber\\_Crime\\_Law\\_and\\_Practice.pdf](https://www.icsi.edu/media/webmodules/publications/Cyber_Crime_Law_and_Practice.pdf)

three culprits in Pune. In investigation CBI found that they had misused the credit card details of one hundred customers. One of the bank customers received a SMS based alert message for purchasing the air ticket by him which was actually not booked by him. The credit card holder felt fishy so he made an enquiry to the bank later he found to know that it was misused. Police requested for the log details for the purchase of an online ticket and police collected the information from the private institution after investigation. Institution revealed that the details of unauthorized transactions used for booking air tickets were found from the State Bank of India. Later after inquiring about those three culprits they came to know that Shaikh who was employed by State Bank of India was posted in the credit card department in the bank, he collected the credit card details of those customers and passed it to his friend kale. Kale in return passed that information to his other friend Lukkad and by using those card details Lukkad booked tickets then he further used to sell the same to other customers and collect the money. In eight days Cyber Cell caught the culprits and further made other banks alert regarding the same.

**Indian first case of ATM Fraud:**<sup>495</sup>

The Chennai City Police arrested Deepak Pream Manwani, 22 years old who was involved in an international gang for committing cyber fraud. Accused had 7.5 lakh; he robbed from two different ATMs also he had broken the ATM in Mumbai and collected 50, 000/- cash. Deepak Prem Manwani was an MBA college drop-out from Pune and he was working in Chennai as a market executive. “One day while browsing the net he got attracted to a site when going further surfing it has offered him assistance in breaking into the ATMs. He contacted the number, it was somewhere in

---

<sup>495</sup>ATM Frauds in India evolved during Digitization URL: <https://indiaforensic.com/atmfraud.htm>

Europe and they provided him with different American Bank credit card numbers at \$5 per card. They also offered magnetic codes for cards for \$200 per code.

Fraudsters created a site similar to that of genuine one so that they can obtain personal bank information with a cheating motive. The visitors believed the site to be genuine, it was logged by the subscriber to get back the money, but in the process of receiving the money fraudsters were collecting customers PIN numbers.”<sup>496</sup> Deepak along with many others entered into the deal and they were ready to hack the bank ATMs, and started gang systematic looting. Manwani created 30 cloned plastic cards enabling him to break ATMs.<sup>497</sup>

In the case of **Citi Group Inc. and Others v. Citi Finance Service and Another**<sup>498</sup> **In State Bank of India (Code No. 05604) Through Its Branch Manager, RRL Jorhat Branch, District-Jorhat-785006 Assam v. Dr. J.C.S Katakya NH-37, At Road, Near Neist Gate No. 1, Jorhat Assam,**<sup>499</sup> the revision petition has been filed under section 21(b) of the Consumer Protection Act, 1986 against the impugned order dated 23.08.2016, passed by the Assam State Consumer Disputes Redressal Commission in First Appeal No. 33/2015, “State Bank of India v. Dr. J.C.S. Katakya”, vide which, while dismissing the appeal, the order dated 13.08.2015, passed by the District Consumer Disputes Redressal Forum Horhat.

The Facts of the case: the complainant is the holder of a savings bank account No. 10354169732 with ATM facility in the RRL Jorhat Branch of the State Bank of India. Somebody claiming to be calling from the Mumbai office of the State Bank of India, telephoned the complainant at 8.00 PM on 08.08.2012, stating that his ATM card had

---

<sup>496</sup>[www.icsi.edu](http://www.icsi.edu)

<sup>497</sup><https://indiaforensic.com/atmfraud.htm>

<sup>498</sup> 2019 SCC Online Del 11589

<sup>499</sup> 2017 SCC Online NCDRC 1093

been upgraded and provided him with new number which will be valid from August 2012 to August 2016 and the PIN will be sent through email and that his old ATM card had been blocked. After some time on the same day, the complainant received a message on his mobile phone that his ATM card has been used for purchase worth Rs. 976/- and a similar message of purchase worth Rs. 796/- was also received thereafter. The complainant transferred the remaining amount in his account to his account in the State Bank of India through internet banking. On making verification, he found that his savings bank account had been debited with another amount of Rs. 28,949/- but no message had been received pertaining to the said amount.

The next morning, the complainant contacted the SBI branch at Jorhat and on their advice, lodged an FIR with Pulibar Police Station. The case was registered under section 420 IPC. After investigation, the police gave a report that they could not trace the culprit and they submitted the same to the court. The complainant approached the banking ombudsman as well but they informed him that the complaint had been closed. In the written statement filed before the District Forum, the OP Bank states that there was no record or evidence of any call made or SMS sent to the complainant by them. The District Forum after considering the averments of the parties, concluded that a sum of Rs. 30,694/- has been debited from the account of the complainant in the State Bank of India by unknown miscreants, without the knowledge of the complainant. The District Forum found banks' deficiency while delivering their service on the part of the Bank in not trying to trace out the transaction so the Forum ordered that a sum of Rs. 30, 694/- with interest @ 10% p.a. should be paid to the complainant along with a compensation of Rs. 20, 000/-

Similarly, in **Rubi (Chandra) Dutta v. United India Insurance Co. Ltd.**,<sup>500</sup> the Hon'ble Supreme Court stated that it was the duty of the Bank to have carried out the necessary verification in the matter, rather than washing their hands off from the whole episode. Evidently, there has been deficiency in service on the part of the Bank, vis-à-vis, the consumer/complainant. Therefore, it is held that the consumer for the below has made a correct appreciation of the facts and circumstances on record while deciding the complaint in favor of the complainant. Moreover, it is a settled legal proposition that the powers in the exercise of the revisional jurisdiction are used only if there is a jurisdictional error or material defect in the orders passed by the consumer.

While going through all the discussion of both the parties the State Commissioner held that there is no merit in this revision petition and the same is ordered to be dismissed and the order passed by the consumer for the below are affirmed. The OP Bank is directed to make payment of the amount in question to the complainant within 4 weeks from today. There shall be no order as to costs.

In 2005, "**Pune Citibank Mphasis Call Center Fraud**,<sup>501</sup> an ex-employee committed fraud on US Customers of Citibank to the amount of Rs. 1.5 crores. The amount transferred by accused to the customers of the United State through internet banking. After obtaining the PIN number of their internet banking he later used in committing the fraud. The case involves unauthorized access for making fraudulent

---

<sup>500</sup> (2011) 11 SCC 269

<sup>501</sup> <https://bnwjournals.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/>

transactions. Section 43(a) of IT Act, 2000 applies in these cases. The accused was found liable under Section 66, 420, 465, 467, 471 of Indian Penal Code, 1860”<sup>502</sup>

In **Aayush Kumar v. State of Bihar**<sup>503</sup> since the petitioner against whom the allegations of fraud in financial transaction through the Internet from the bank account of the petitioner was already in custody. After investigation the police has not found any direct evidence against the petitioner and he was used by the two other co-accused for getting an account opened in his name but the transactions in the same was not within his knowledge. The court after having considered the facts and circumstances of the case let the petitioner be released on bail upon furnishing bail bonds of Rs. 25,000/-(twenty five thousand) with two sureties subject to the conditions (i) that one of the bailers shall be a close relative of the petitioner, (ii) that the petitioner and the bailers shall execute bond with regard to good behavior of the petitioner, and (iii) that the petitioner shall also give an undertaking to the Court that he shall not indulge in any criminal activity. Any violation of the terms and conditions of the bonds or the undertaking shall lead to cancellation of his bail bonds. He also needs to be present before the court on each and every date without any failure. If fails to do so it shall also lead to cancellation of his bail bonds.

Indian judiciary system is not being able to deliver proper justice to the citizens in the absence of specific legislation or statute that covers cyber fraud. The accused are not getting strict punishment for the act they had committed for this reason the cases are on the rise every day. The case of phishing was brought before of Indian law even in the absence of specific legislation on phishing.

---

<sup>502</sup>Kumudha S & Rajan Aswathy, A Critical Analysis of Cyber Phishing and its Impact on Banking Sector, International Journal of Pure and Applied Mathematics, Volume 119 No.17 (2018) URL: <https://acadpubl.eu/hub/2018-119-17/2/128.pdf>

<sup>503</sup> 2020 SCC Online Pat 684



In the case of **National Association of Software and Service Companies v. Ajay Sood and Ors**,<sup>504</sup> the accused Ajay Sood and Others (Operators of a placement agency involved in head-hunting) he created email and sent it in name of NASSCOM Company and sent it to third. The judgement was delivered on 5th March when the ‘Phishing’ scam was considered to be an illegal in India Act, entailing an injunction and recovery of damages by Delhi High Court. The court stated that perpetrators to commit cyber fraud pretend to be legitimate officers of an association to get internet banking username and passwords, debit or credit card details etc. The personal details collected by using fake identity so that he can collect the identity of legitimate parties to take collective advantage. Court held with Phishing involves fraudsters who conform themselves as representatives from banks and make an unauthorized transactions of cash from e-banking accounts after tricking the victim to gain confidential access to their bank account. The Court stated that in absence of specific legislation in India for penalizing phishing as an offence, would lead to misstatement creating confusion for the source of its origin of the email which may be intending to farm the victims and their identity.

The National Association of Software and Service Companies (NASSCOM), India’s software association was the plaintiff in case. “The defendant sent scam mails in the name of NASSCOM to access the account details. The Court restrained defendant from using the name NASSCOM.”<sup>505</sup>

While conducting an investigation it was found that the defendant was sending offending emails from different fake email accounts as created by him to avoid any kind of legal actions. Accused deleted all the contains and fake names used by him.

---

<sup>504</sup> 119 (2005) DLT 596

<sup>505</sup><http://legalserviceindia.com/legal/article-3210-cyber-crime-a-hindrance-in-digitalworld>

At last the defendants confessed his illegal activities and they were held liable to pay Rs. 1.6 million compensations for loss and the hard drive was given back to the plaintiff as they were the real owner.

This judiciary obtained a new milestone by making phishing as an illegal act without the specific legislation placed for the said offence. This case made IP owners to have faith in the ability and willingness of the legal system.”<sup>506</sup>

In **Umashankar Sivasubramanian v. ICICI Bank, Petition No. 2462 of 2008**,<sup>507</sup> the Adjudicating Officer under the IT Act at Chennai was deciding a dispute pertaining to phishing. The petitioner filed application for Adjudication under section 43 read along with section 46 of the Information Technology Act 2000. The petitioner is the NRI Indian who was employed as a Process Engineer, Dept: SUFEMS, ZAKUM Development Company in Abu Dhabi. The petitioner had a bank account in ICICI Bank, V.E. Road, Tuticorin. In August 2007, Petitioner account balance was Rs.6, 20, 846/-. Customer received mail for a security update from *customercare@icicibank.com* but the petitioner was surprised to know that his account was debited from the bank account.

The petitioner denied any transfer of inquiry from ICICI Bank regarding the transaction. The bank suggested filing a complaint to Customer Care within 24 hours. The police indicated the possibility of the Bank or some of its staff being behind the fraud. The petitioner requests the police to initiate action against the ICICI Bank and retrieve the money. This petition was subsequently transferred to the Cyber Crime Police Station at Chennai.

---

<sup>506</sup>Crimes in Cyberspace: Right to Privacy and Other Issues - Academike (lawctopus.com)

<sup>507</sup> [https://www.naavi.org/cl\\_editorial\\_10/umashankar\\_judgement.pdf](https://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf)

The Adjudicating Officer held that the ICICI Bank failed to exercise due diligence by not preventing “unauthorized access,” as contemplated under Section 43. The tribunal recognized the imbalance of power between the Bank and its customers, and held that terms and conditions governing Internet Banking appearing on the website of the Bank in the fine prints cannot absolve the Bank from its liability of providing adequate security measures so that requirements of the Act, the rules and regulations made there under are met satisfactorily and the customers’ interests are well protected. Thus the respondent bank namely ICICI in the instant case is directed to pay a sum of Rs. 12, 85, 000/- (Rupees Twelve Lakhs Eight Five Thousand only) to the petitioner within 60 days from the date of issue of this judgement.

In **State Bank of India v. Chander Kalani & Ors.**,<sup>508</sup> the Telecom Dispute Settlement and Appellant Tribunal (TDSAT), New Delhi was adjudicating a dispute pertaining to alleged hacking of the complainant alleged that the bank, i.e. State Bank of India (SBI) was negligent in disclosing details of the complainant’s bank account by responding to fake emails and was therefore liable to pay the complainant compensation under Section 43A of IT Act 2000.

Telecom Disputes Settlement and Appellate Tribunal (TDSAT) held that “on a careful reading of Section 43A, it is absolutely clear that the negligence while implementing and maintaining reasonable security in bank practices and procedures alone creates a liability to pay damages or compensation under Section 43A, if such negligence has caused wrongful loss or wrongful loss or wrongful gain to the person affected.

In “**Bank NSP Case**, where a trainee of management used to exchange email messages using the computer of a company. The girl has used fake mail ids

---

<sup>508</sup> Cyber Appeal No. 13 of 2015 (m. A. No.282 of 2017)

“Indianbarassociations” through computer of company to the foreign client of boy’s company the court held the bank liable for sending email from their computer system”.<sup>509</sup>

In **Ali Ibrahim vs. the State of Kerala on 14 October 2014**,<sup>510</sup> the court stated that, since the fraud is being committed involving communication via email, telephone call, and online bank transaction it should be possible to verify the money trail. Since the bank has to adhere to Know Your Customer (KYC) norms and they must be in position to say to whom and to which address the money was transferred. Investigation on ATM fraud is relevant. Bank must cooperate with the police for investigation. If banks are not following KYC norms then the extent of liability of the bank will increase. To conduct a thorough and effective investigation than the investigating agency should inter alia have:

1. Adequate technological assistance
2. Competence to investigate the money trail
3. Competence to investigate the telephone trail
4. Ability to carry out investigation in different States.

CBI has an Economic Offences Division- for investigation of major financial scams and serious economics frauds, including crimes relating to Fake Indian Currency Notes, Bank Frauds, Cyber Crimes as well as a Special Crimes Division for investigation of serious sensation and organized crime under the Indian Penal Code and other laws on the requests of State Governments or on the orders of the Supreme Court and High Courts.

---

<sup>509</sup>[http://www.indiancybersecurity.com/case\\_study\\_the\\_bank\\_nsp\\_case.php](http://www.indiancybersecurity.com/case_study_the_bank_nsp_case.php)

<sup>510</sup> <https://indiankanoon.org/doc/72673147/>

It seems CBI would be the best choice for a thorough and effective investigation. However in the instant case the grievance of the complainant appears to be of a private nature and the amount he is said to have lost is about Rs. 68 Lakhs. No public officer is alleged to be involved in the matter and there is no loss of public funds.

The court further directed that the investigation shall be supervised by a senior officer preferably of the rank of Inspector General of Police or Deputy Inspector General of Police as may be nominated by the Additional Director General of Police (Crime) and the said office shall closely and intensely monitor and supervise the said further investigation. It was also made clear that the court has not made any final pronouncement on the necessity of entrustment of investigation to the Central Bureau of Investigation and depending on the outcome of the investigation they said the issue will be further considered.

In **Tony Enterprise v. Reserve Bank of India on 11 October 2019**,<sup>511</sup> the accused used a new form of technique to commit fraud i.e. by using SIM Swap fraud where they used duplicate SIM issued by a mobile service provider against the registered mobile number. Through this duplicate SIM they will receive One Time Password (OTP) generated by the bank to get access for making unauthorized transactions. In this case the police investigation established that fraud has been committed and the accused belong from West Bengal. There was no mistake on the part of the petitioner. The police investigation enclosed the details that the accused committed fraud through the SIM Swap by obtaining duplicate SIM card of the Petitioner from the mobile service provider and after making unauthorized transaction he immediately withdrawal of the amount from ATM in West Bengal.

---

<sup>511</sup> <https://indiankanoon.org/doc/73091604/>

The Court focused on the master circular issued by Reserve Bank of India dated 6.7.2017 protecting the customer on the unauthorized electronic banking transaction.

The circular stated zero liability of the customer:-

“i. if the bank is liable for having contributory fraud or negligence while providing their banking services and the deficiency in the part for unauthorized online banking transactions.

ii. If it is matter of third party breach and bank is deficient in providing adequate services in its banking system, and the consumer inform the bank within three days without any failure about unauthorized online transaction.”<sup>512</sup>

So in such cases where both the bank and customer are not liable for the loss then the question arises for the remedy to the bank as to whom the bank approaches for the loss which they had suffered. Since banking is a contract among the banker and customer so it is the bank's duty to protect the interest and confidentiality of the customer's account details in all matters. Even though the bank had devised Secured Socket Layer (SSL) for online transaction which is encrypted even though it can be hacked using different modes or methods. It is bank duty to secure their customers safety.

With the adoption of internet banking which is considered to be one of the easiest and safest ways for completing transactions there has been a rise of e-payment fraud. ATM fraud by obtaining ATM details by the fraudster is one of the common means of conducting fraud. In such cases the issues arise as who will bear the liability of loss to the customer, is it the bank who is responsible for the security of the money

---

<sup>512</sup>Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions URL: Reserve Bank of India - Index To RBI Circulars

transaction or is it the service provider who provides the master/visa card or debit/credit card.

**“AboladeBpde v. First Bank of Nigeria Plc. &MasterCard West Africa Limited,** delivered on 10 April 2019, is a case of unauthorized electronic transaction. The plaintiff lost cash from his account with the involvement of MasterCard information i.e., fraudulent transaction by misusing card details. The court in this case relied upon the doctrine of privacy of contract which arises out of a banker relationship with their customer about the guidelines provided to the card holder of the bank while providing card facilities to their customers.” The court held that in case of unauthorized electronic transaction from the account, then the bank bears the liability for such transaction and the MasterCard Company will not be liable for such transactions. Plaintiff has issued against the bank and the MasterCard Company for his loss that occurs. The Court held that MasterCard being the technology provider company so it can be liable for the unauthorized transactions. It is the duty of the bank to provide security to the customer account and identity so the bank will be held liable for the loss of customers.”<sup>513</sup>

**Guaranty Trust Bank v. Motunrayo-Tolulope Aloegen (nee Oyesola)**<sup>514</sup> In that case, the defendant had a defence that the Master Card was liable. The court after looking through the circumstances denies the defence of the defendant and the defendant was held liable as no cause of action was found against MasterCard.”<sup>515</sup>

---

<sup>513</sup> *Supra* note at 513

<sup>514</sup> Guaranty Trust Bank v. Motunrayo- Tolulope Aloegen (nee Oyesola), unreported SUIT No: CA/L/461/2016 delivered on 1 March 2019

<sup>515</sup> *supra* note 448

**Justice K. S. Puttaswamy v. Union of India**,<sup>516</sup> Justice K.S. Puttaswamy (Retd.), judge of the Madras High Court, Challenged the constitutional validity of Aadhaar Scheme. He urged that the scheme of Aadhaar violated the right of privacy which has been guaranteed by Part III of the Constitution of India. It was held that right to privacy is a fundamental right under Article 14, 19 and 21 of the Indian Constitution.

Facts of the case:- Aadhaar Card i.e. Unique Identification Authority of India (UIDAI) was a scheme to project the BPL (Below Poverty Level) family. In January 2009, the Planning Commission of India passed a notification on UIDAI and in 2010; the National Identification Authority of India Bill was passed by the Commission. Retired Justice K.S. Puttaswamy and Mr. Sharma filed PIL Writ Petition before Supreme Court of India in 2012 challenging the validity of Aadhaar. The UIDAI scheme was challenged on the ground that it was violating the fundamental right of the citizens of India i.e., Right to Privacy under Article 21. Aadhaar was passed in 2016.

“The Supreme Court held that the right to life and personal liberty has also included Right to privacy.<sup>517</sup> If the conduct of cybercrime violates the individual personal property or their belonging then the court will convict the accused for the violation of Article 21 of the constitution of India and will be charged accordingly.”<sup>518</sup>

**Jagdeo Singh v. The State and Ors**,<sup>519</sup> this case is all about admissibility of digital evidence before the court. It is a matter of admissibility of telephone calls in CD in

---

<sup>516</sup> (2017) 10 SCC 1

<sup>517</sup>Article 21 of Constitution of India: Protection of life and personal liberty- No person shall be deprived of his life or personal liberty except according to procedure established by law

<sup>518</sup>India : Revisiting the Current Scenario of the Safeguards for Cybercrime URL: <https://www.lexology.com/library/detail.aspx?g=27a808e5-003d-4588-bbf1-c400a4c15b30> (visited on 10.8.2020)

<sup>519</sup>Jagdeo Singh v. the State and Ors (MANU?DE/0376/2015)



the absence of certificate as mentioned under section 65B of Indian Evidence Act. The High Court held that the admission of secondary evidence before court proceedings is not admissible as electronic evidence and electronic evidence is not admissible without certificate from the authority and cannot consider the same in any other purpose. In another important judgement of Delhi High Court in the case of **Dharambir v. CBI**,<sup>520</sup> held that compliance to Section 65B is mandatory to active accessible information as where the data were originally stored.

In **DAV Public School v. The Senior Manager, India Bank, Midnapur Branch & Ors.**,<sup>521</sup> the Principal of the DAV Public School has filed a complaint regarding deficiency of banking services against the Bank. DAV Public School has opened an account in their bank without a net banking facility but the account was linked with CIF (Customer Information File) of the Principal Mr. Sanjiva Kumar Sinha. The plaintiff has sent staff for an update of the bank passbook but it was not done on the particular day due to technical problems as mentioned by bank staff and the next day the passbook was updated but unfortunately it was found that they have lost Rs.30,00,000/- from the account. Plaintiff's mobile was not working for 5 to 6 days he thought it was the network problem but now it came to know that duplicate SIM was issued to the accused by BSNL service provider, and they ported it to another service provider Bharti Airtel. The transfer of SIM card was made to another persons' name of Sanjay Kumar Sinha who was residing in the same address in replace of Sanjiva Kumar Sinha, thereafter they withdraw the money posing they were the right account holder.

---

<sup>520</sup>Dharambir v. CBI 148 (2008) DLT 289

<sup>521</sup>DVA Public School v. The Senior Manager, India Bank, Midnapur Branch & Ors. CIVIL APPEAL NO 9352 of 2019 URL: [https://main.sci.gov.in/supremecourt/2018/28537/28537\\_2018\\_8\\_1502\\_19253\\_Judgement\\_18-Dec-2019.pdf](https://main.sci.gov.in/supremecourt/2018/28537/28537_2018_8_1502_19253_Judgement_18-Dec-2019.pdf)

It was specific from the part of school that they never approach banks for internet facility for the transaction of money. The first unauthorized transaction of Rs. 25,00,000/- was done on 9.9.2014 and before the bank would block the account again, the second unauthorized transaction of Rs. 5,00,000/- was done from the school's accounts. Thus, gross error was on the part of the Bank for the unauthorized transaction of money from school's account. It was the clear case of deficiency on the part of Indian Bank. Bank was held liable for the negligence on their part. The court held that both the parties are jointly responsible for the loss of money, so the bank was directed to pay half relief of Rs.10, 00, 000/- to the complainant.

Reserve Bank from time to time issued guidelines in order to run the banking industry smoothly considering the security of their customers. But in every case banks are found liable for not performing their duty, negligence is always found in the part of the bank with the involvement of bank staff. Banks are not following the guidelines appropriately issued by RBI for the safety and in order to control the bank frauds.

As in the case of **ICICI Bank Ltd v. Official Liquidator of APS Star Industries Ltd**,<sup>522</sup> the court held that when a delegate is empowered by Parliament in order to enact a policy as well as to issue directions, they have a statutory force. Reserve Bank of India is a delegate, so RBI issuing such guidelines or policy has statutory force. Such guidelines/ policy issued by RBI need to be read as supplement to the provisions of the Banking Regulation Act, 1949. The banking policy is enunciated by RBI, such policy cannot be said to be ultra virus the act.

---

<sup>522</sup>(2010) 10 SCC 1

In **N. V. Subba Rao v. State of Andhra Pradesh**<sup>523</sup> a case was registered against the Manager of Bank Sh. V. N. Subarao, the then Manager, Central Bank of India and Sh. Attur Prabhakar Hegde, Prop of M/s A. P. Enterprises for the offence punishable under Section 120B read with Section 420 IPC and Section 420, 468 and 471 read with Section 468 IPC and Section 13(2) read with Section 13(1)(d) of the Prevention of Corruption Act, 1988 alleging for misusing his official position as a public servant and entered into a criminal conspiracy with Attur Prabhakar Hegde and defrauded the Bank amounting Rs.1.168/- crores by sanctioning temporary overdrafts and term loans to various individual.

After investigation CBI filed charge sheet against both the accused persons in the court of the Special Judge for CBI Cases at Visakhapatnam which was numbered as CC No. 8 of 1998. In charge sheet they were alleged that while functioning as branch Manager he dishonestly disbursed 494 loans of Rs.10, 000/- to the employees of Railways and other organization as he was instructed by his controlling officer to disburse loans only after obtaining undertaking from their employers that the monthly installment of repayment of loan will be deducted from the salaries as primary security and also mortgage on the plots sold to the borrower through the Prop M/s. A. P. Enterprises.

An amounting to Rs.49,40,000/- and credited the proceeds to the account of the Proprietor without obtaining the requisite undertaking from the employers and without proper security of monthly installments to be deducted from their salaries. Out of 494 borrowers, 45 persons have been identified by the prosecution M/s. A. P. Enterprises after having received the proceeds fraudulently and dishonestly did not

---

<sup>523</sup> Through Inspector of Police, CBI/SPE, A.P. Criminal Appeal No. 1688 of 2008 with No. 1700 of 2008 decided on December 3, 2012 (2013) 2 SCC 162

get 45 plots registered in their names not the borrowers have the loan amount from the bank.

The Special Judge for CBI cases, Visakhapatnam sentenced both of accused for one year rigorous imprisonment<sup>524</sup> and to undergo RI for a period of two year along with a fine of Rs.5,000/-, in default, to further undergo simple imprisonment for 3 months for the offence punishable under Section 420 of Indian Penal Code, 1860. Manager was further sentenced to undergo imprisonment for three months in lieu of offences punishable under Section 13(1)(d) of Prevention of Corruption Act, 1988.

They further made an appeal before the High Court of Andhra Pradesh at Hyderabad as a case of N.V. Subarao v. State of Andhra Pradesh.<sup>525</sup> There was wrongful loss to the Bank as well as to the purchasers and being Bank Manager could not be his responsibility to someone else. Bank set up a departmental enquiry against the conduct of the Bank Manager accordingly he was dismissed from the services. However, the decision of departmental enquiry was not helpful to the court and the court held that offence of criminal conspiracy has been proved by circumstantial evidence; consequently both the appeals fail and appeal are accordingly dismissed.

“An Indian origin man is sentenced for three year and four month in the UK for allegedly committing a cyber fraud operation by stealing ten thousand pound from the victims. Abhay Singh 33 year old was arrested by Metropolitan Police Central Specialist Crime unit Officers for the charge of conspiracy to conceal, disguise, convert, transfer and remove criminal property and he was sentenced at Birmingham Crown Court. Specialist Crime unit Officers have seized many suspicious items such

---

<sup>524</sup>Section 120 of Indian Penal Code, 1860 vide judgment & order dated: 30.4.2009

<sup>525</sup> Criminal Appeal No.602 of 2001 decided on 29.1.2008

as driving licences and bank cards along with large sums of cash. Their group has stolen ten thousand pound from different individuals, businesses, schools and many other organizations. In their course of action they had not considered any livelihood of public members or the future of some business during the course of their action.

This case was a highly complex case including investigation against cybercrime and money laundering organized crime groups. This accused conducted acts of cyber fraud and money laundering operation since January 2016 and January 2019. They said that cyber fraud should not be underestimated because of its impact on every individual including the economy as a whole.”<sup>526</sup> In **Ostern Pvt. Ltd. & Anr v. State of West Bengal &Ors**,<sup>527</sup> the Calcutta high court dealt with cyber hacking in the banking sector. Where the petitioner mail account being hacked and substantial sums are transferred by fraudster from his account through hacking the banking system. The banking system was totally hacked and under the control of hackers. Customer did not receive any of the alert messages of fraudulent transactions from his account. The court held the bank liable for the mistake of their authorities and also punished the fraudster.

**Puneet Mittal v. State Bank of India Order dated 31st January, 2015**,<sup>528</sup> is a suit for recovery of Rs. 90,000/- along with the interest for the unauthorized ATM withdrawal. Plaintiff hold a Saving Bank Account with bank bearing no. 10786738903 at the Green Park Extension Branch from the last 25 years and ATM

---

<sup>526</sup>India Today Dated: December 5, 2019 URL: <https://www.indiatoday.in/crime/story/indian-origin-man-jailed-cyber-fraud-uk-1625267-2019-12-05m>

<sup>527</sup>Ostern Pvt. Ltd. & Anr v. State of West Bengal &Ors, AIR 2014 URL: <https://www.casemine.com/judgement/in/5ac5e3fa4a93261a672cfd6c>

<sup>528</sup>Puneet Mittal v. State Bank of India on 31 January 2015 URL: <https://indiankanoon.org/doc/159148066/>

cum Debit Card no.6220180106500075630 was also issued to the plaintiff by the bank.

The plaintiff on 27.07.2012 received two messages at 8.12 am about the ATM Card being used at Majestic, Bangalore with the transaction of Rs. 40, 000/- in two transactions while the ATM card was still in possession of the plaintiff back in Delhi. Immediately after the message plaintiff changed the PIN number and took a mini statement and found Rs. 40,000/- transactions from plaintiff's account at MG Road, Bangalore. Plaintiff did not receive any message for those two transactions so he made a complaint at the helpline jumper of the bank. A written complaint was lodged with Deputy Commissioner of Police, Hauz Khas. Written complaint was moved at the bank on the same date and the card was blocked.

It is the grievance of the plaintiff that the defendant bank was the custodian of the plaintiff's account and the bank is liable to prevent any fraudulent or unauthorized withdrawal of the amount. Notice seeking demand of the amount of Rs. 80,000/- with 18% interest was issued upon the defendant on 01.11.2013. Hence, the present suit was filed seeking Rs.80,000/- from the bank along with the interest amounting Rs. 10,200. Therefore its suit for recovery of Rs.90,200/- from the bank.

The defendant was unable to establish the fault of the plaintiff in the entire transaction. Therefore, no fault was found on the part of the plaintiff. The Court held that a bank being custodian of the accounts of the customer is their responsibility to secure their account from fraudulent or unauthorized transactions. Therefore the bank is held liable for such fraudulent transactions and the loss incurred by such transactions.

In “**Himanshu Sarkar v. State Bank of India & Another**,”<sup>529</sup> Himanshu has filed a complaint at Bowbazar Police Station about the fraudulent transaction. He is an account holder in State Bank of India bearing account number- 20010244005 at Sashi Bushan Dey Street Branch Kolkata with ATM facility. On the day of the incident, Himanshu (complainant) went to an ATM at Subodh Mallick Square, Kolkata for withdrawal of money. Due to technical problems it was unable to dispatch the money from the ATM even after completing all the steps. Thereafter he went to another SBI ATM corner at Rafi Ahmed Kidwai Road, Kolkata and withdraws Rs. 2,000/- he came to know his account has already withdrawn Rs. 10,000/- at previous SBI ATM corner. He went to Bowbazar police station to file FIR. He knew that it was difficult to get his money back, he then gave notice to the bank about the fraudulent transaction and sought the bank to take appropriate action and made requests not to delete the CCTV footage of the ATM corner on the particular date of incident. The Court held the bank liable by their deficiencies in performing their duties properly and the bank should pay Rs.10,000/- along with 8% interest from the date of fraudulent transaction done by hacker. Further, the bank must refund the amount to the complainant within 30 days.”<sup>530</sup>

---

<sup>529</sup>Himanshu Sarkar v. State Bank of India & Another District Consumer Disputes Redressal Commission (19 August, 2014)

<sup>530</sup> URL: <https://www.casemine.com/judgement/in/590a09f04a932663936d1078>

## **CHAPTER SIX**

### **CONCLUSION & SUGGESTION**

The fraud in the banking sector has been a key concern to the banking regulator as well as to the government. Adoption of advancement in banking technology has created convenience to the customer and it has made vulnerabilities to the customers' security. It has been challenging to combat technology crime i.e. cyber fraud which is targeting the economy as a whole. Fraud has never been higher on the agenda before the emergence of cyber fraud, there is a clear need for the banks to come together in order to work for the agenda of compliance, legal, fraud control, and security mechanism. Technology has made us to be more dependent on them, especially for performing banking business. Banks are providing different electronic services by making it more proficient and convenient to their customers. Evolution of the internet has transformed the banking sector; it brought an escalating swiftness in banking business. Almost all of the banks have already implemented the internet banking facilities and these are beneficial to both banks as well as customers. The changes brought by the banking system decline the hassle or transaction cost and even save time of customers. Banks with the technology adoption provide better customer facilities, now people are taking full advantage of such banking services. Banks have provided different platforms for performing internet banking transactions such as credit/debit card, mobile banking, Paytm money transaction using UPI number etc. Adoption of digitalization in government as well as banking sector there is rise of cyber fraud. With the expansion of services the new digital crime of cyber fraud is creating serious challenges in the absence of a dedicated legal framework on cyber fraud. There is vulnerability of information which is available in computers or the



internet so the rapid development of technology is posing a threat to that information, leading to the challenges of their security.

Cyber fraud is one of the cybercrimes conducted through the use of computers and the internet by targeting computers or using a computer as a medium. Cyber fraud affects the modern quality of life of individuals or banking institutes, but also hampers economic growth. In absence of a legal framework there is no specific definition of cyber fraud so that we can understand to what parameter does it constitute cyber fraud. There is difficulty in illustrating the definition now which it's becoming a key analytical problem. Banking System is having both benefits and challenges after the adoption of upgraded technology in delivery channels of banking. With the admittance of time there is change in conducting crime, at time of regulating Information Technology Act, 2000 those crimes such as cyber fraud or unauthorized electronic banking transaction were not found so it got over lapsed. But now Cyber fraud is rising at an alarming rate so looking into the necessity of the present situation there is a need for enactment of law which can appropriately regulate internet banking. We cannot expect law to remain rigid, with the change of technology and necessity of the situation the only Cyber Law of India i.e. Information Technology Act, 2000 (amendment Act 2008) once again need to be amended and include cyber fraud crime within the ambit of the legislation. Inefficiency of enacted law has proven their inadequacy and vulnerability while governing internet crime. The insecurities of the individuals about the security of their accounts and privacy have created complexity in banking business. The growth of cyber fraud in electronic banking has completed the law enforcement for the applicability of law. This cyber fraud is not only affecting the banking sector but it is even affecting individuals that hamper the growth of countries' economies. Cyber fraud is considered to be white-collar crime, it

often makes headlines in daily news whose growth is rapid with the development of technology and it constitutes one-third of all cybercrimes. The fraudster conduct the fraud by misusing credit card by hacking their passwords, skimming ATM cards, vishing, sending emails, SMS in a way of phishing, or by calling an individual's proclaiming themselves as a officer of the particular bank making an excuse such as update of KYC or for the renewal of the ATM card or even sometime they will claim the individual customer as a winner of lucky draw or winner of Kaun Banega Crorepati (television show). They will convince the customer to follow their instruction to download certain apps from Google play store and lastly they will ask for OTP saying for authentication of the registration or verification. So in this manner they complete their transaction process and empty the consumers' account. A very low number of victims notify the bank of unauthorized electronic transactions and file a complaint in a police station. The victims do not find themselves comfortable disclosing the fact of being victim of cyber fraud may be because of the lack of confidence, trust, image consciousness, and business in a society.

Internet banking is just an extension of traditional banking shifts by different ways of delivering their services for the convenience to their customers. In order to deal with the challenges of cyber fraud in India, no statute till date provides a specific definition of cyber fraud; it has been problematic for law enforcement agencies to convict the fraudster of cyber fraud. Reserve Bank of India being the central bank to all the banks in India provides direction in order to regulate banking business in India. RBI time and again issues different circular and notification in order to secure the customer interest and bank account from the internet fraud. With the failure to provide security for their customers there has been a rise in the question of adequacy of law dealing with technology driven situations. It shows the existing enacted laws of India are

inadequate in dealing with the challenges laid by cyber fraud in the electronic banking system. It's getting more complicated, unable to provide surety about the safety of their accounts with the increasing fraudulent activities in the society. Therefore, apparently new law needs to be framed for efficient handling of internet banking and the intangible nature of cyber fraud evidence. In Indian it is necessary for all the banks to obtain license from the Reserve Bank of India and under Banking Regulation Act, 1949 no person other than a banking company or institute notified by the central government are authorized to accept the deposit or withdrawal. Information Technology, 2000 amendment Act 2008 has made changes in Indian Contract Act, 1872 and further added e-contract as a valid contract after fulfilling the requirement for making it valid. E-contract is paperless electronic contract born out of present needs for suitability and efficiency of services for the customers.

Eventually e-contract is conducted to complete e-commerce through electronic means by validating and authenticating the contract by using digital signature. The substantive aspects of Indian criminal laws are covered by Indian Penal Code, 1860. Generally, cyber fraud is an act of deception in order to secure something through the medium of the internet. Indian judiciary in order to provide verdict in case of cyber fraud they consider similar kinds of traditional offences such as cheating, dishonestly, fraudulently under Indian Penal Code. IT amendment Act, 2008 has brought changes in IPC by adding new sections for penalizing certain cyber offences such as forgery of electronic records, destroying electronic evidence, etc.

In India there is no uniformity of Cyber law as that to European Union. The Budapest Convention is an important international convention on cybercrime; it provides uniform cyber law within their member state. The Convention acts as guidelines to

other states so that they can formulate their own domestic law so that it will be convenient for them to tackle the challenges. After studying different acts of India it is clearly proved there is inadequacy of enacted law and they must reconsider cyber fraud as a cybercrime so that they can include a section for definition of cyber fraud and decide the punishment for this particular offence, so that judiciary can act more confidently and wisely during its verdict. Cyber fraud being not included in IT Act, 2000 it creating difficulties in procedure of investigation. Cyber fraud being a borderless crime it's being more difficult to locate the jurisdiction of the particular offence. Investigating process is getting delayed in absence of coordination among the states. There is a need for a Mutual Legal Assistance agreement so that we can collect the information from foreign states within time because the electronic evidence is fragile in nature, it can be easily destroyed so, in order to present the e-evidence before court within the stipulated time.

In the present scenario fraudsters are more advanced so they are two steps ahead then the investigating officers/authority dealing with cyber fraud. Even though Indian Government has appointed an agency i.e., Indian Computer Emergency Response team, it is still not sufficient. The members or officers of this CERT-In team must be expertise who can handle the emergency call of cyber fraud without waiting for other computer expertise to crack the system. Cyber Police should be trained separately; they must be having subject background like computer, Information Technology, Forensic Science because this department needs a stronger mind than the body. Every year there is a rise of cyber fraud; consumer security needs to be reconsidered by the legislator.

Internet fraud if considered as business than it's the most profitable and easy earning money. Rampant increase of cyber fraud is becoming more challenging to the cyber police. There are many issues of cyber fraud which need to be taken into consideration for tackling cyber fraud. First issues will always be the definition not being provided by the Information Act, 2000 which is making it difficult to carry forward the investigation of cyber fraud cases. In absence of definition investigation is facing problems since there is no such standard procedure established for search, seizure for cyber fraud. All the direction for investigation of digital crime is totally different from that of traditional crime. Cyber fraud required different guidelines for the investigation since it involves multiple predictors and multiple jurisdictions. Reserve Bank should frame new guidelines considering the consumers interest and security, they must update KYC (Know Your Customer) rules which the bank needs to strictly follow in order to control rising cyber fraud. Most of the online banking fraud involves banks staff, the authority must maintain check balance about their movements from time to time in banks. Bank staff required continuous training sessions about alertness that they are required to maintain. Customers are paying every charge for the services provided by the banks so it's their responsibility to maintain the security of their account details. Cyber Security needs updates because fraudsters or hackers have already shifted their modes of *modus operandi* of cyber crime.

“Jurisdiction provides states with the power and authority to protect the rights and duties of the people and enforce the law against the violation of laws. The jurisdiction for cyber fraud established on the factors like nationality of the fraudster/ offender,

nationality of victims etc.”<sup>531</sup> Jurisdiction is creating difficulties in investigation for collecting digital evidence, because of lack of mutual assistance among the countries. Council of Europe’s Convention on Cybercrime 2001 seeks harmonize law in order to combat cyber fraud in issues of investigating and making international corporations. It acts as guidance to the domestic laws to incorporate their own laws, and provides guidance on mutual assistance as a mutual legal assistance treaty. The cyber frauds reports are just a handful out of the ocean and silence on part of the legislature and judiciary over the issues are creating misunderstanding about their inabilities. Enacted laws are inadequate to deal with the challenges of digital crime so law is in need of change with the advancement of technology in order to create new strengthened Cyber Laws in India. Uniform Cyber Law needs to be framed to create mutual assistance in dealing cyber fraud. Global cooperation is mostly required in order to counter the growing transnational threat of cyber frauds. Under uniform cyber law, international cyber courts need to be established where prosecution can continue with the court case with the evidence which will be applicable for all of the countries. Law should be formulated considering safeguarding the customer’s needs to ensure that laws that create restrictions on the access of the internet should not violate their right to security. Clarity in law is needed to ensure that law is not against the society or individuals.

### **Findings of the Study:**

- Unemployment is one of the major factors of the rise of cyber fraud. Most of the perpetrators of cyber frauds are young graduates who are unemployed but

---

<sup>531</sup> <https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html>

highly knowledgeable in computer systems. This has automatically increased their chances to participate in criminal activities for their survival.

- The lack of strong uniform cyber law encourages the fraudster to commit more frauds knowing that they can always escape the verdict. It being borderless crime makes fraudsters believe that they can escape the punishment, make them too lazy to follow the laws. Government needs to enforce stronger laws so that the judiciary can pass a verdict setting an example before the fraudster that the criminal will not go unpunished.
- The cyber fraud has occurred due of lack of inadequate supervision of banking, inadequacy in banking management, collusion among the staff, presence of weak regulatory agency, lack of appropriate advance tools and technology in banks for early warning detection of cyber fraud, lack of unawareness about the new tactics in computer system used by fraudster among the bank employees and customers inadaptability of precaution measure for safe banking transaction and lack of awareness about security system provided by the enforcement, a lack of coordination between banks to operate across India, delay in legal procedure for reporting and many other are considered to be a major reason for fraud.
- Cyber security must consider the objective of reducing customers' vulnerabilities about their information, collaborate with private/ public and international entities and help them to educate regarding the current trend of information technology about cyber fraud and search the way to obtain effective solutions.

- After studying many articles and case law it has been found that in cases of bank fraud the negligence is found on the part of the bank. Banks are not following guidelines which have been formulated for KYC i.e. to Know Your Customer and it needs to be reframed. Bank staff is involved in most of the internet banking fraud by misusing their position for obtaining the personal accounts details and later on making unauthorized transactions. Banking institutions should provide training sessions to their staff regarding updated operating systems, bank cyber security, and they must also know about the present digital frauds.
- Section 75 of Information Technology is inadequate as well as ineffective when it comes to implementation. Section 75 applies to those who commit cyber offences outside the Indian territory involving computers, computer systems and their networks. The Section 75 may appear to be ineffective when the judgement passed by Indian Court for the extra territorial jurisdiction may not accept the principle by the foreign court when the offence committed outside India relating to computer or computer system may not be an offence under their law of country.
- There is a lack of global uniform legal enforcement standards for the admissibility of digital evidence. The usage of computer networks is accepted world widely, despite the fact of having a different legal system the challenge of admissibility of digital evidence before the court are similar. There are only some countries who have updated their legislation for insertion of digital evidence. Since we all are facing challenges related to the cyber world and coming together is the only solution to this crime so there is a need for binding legal standards.



- There is imperfection of legislation in the sphere of combating transnational cyber fraud. There is still absence of precise clarification of law in case of cyber fraud so it is difficult to interpret and apply the law. There is weak specialized professional training for law enforcement agencies relating to the prevention and investigation of cyber fraud. Conducting investigation measures like search, seizure and arresting computer machinery. Therefore there must be full procedure measures for conducting investigation on search and seizure of electronic evidence and they need some peculiarities and special background.
- Lack of International Co-operation. The internet has provided cyber fraud as an international colour and the central issue for cyber fraud is the jurisdiction. Offender knowingly tries to take advantage of this lacuna. In order to perform effective investigation, firstly they need to check whether there exists a bilateral or multilateral legal instrument referred as Mutual Legal Assistance Treaty (MLAT) treaties among the countries in order to facilitate evidence gathering. Mutual Legal Assistance Treaty (MLAT) saves time and in absence of such legal instruments, it will cause delay in return to make further investigations. India needs to have more multilateral instruments in order to access more assistant in order to fasten the investigation process.
- There is a major lacuna in Information Technology, Act 2000 since it does not cover certain important contraventions and offences as well as technological aspects for cyber or internet fraud. Today Cyber Fraud constitutes  $\frac{2}{3}$  majority of cyber crime, it is comparing individuals as well as the nation at large. India has no such specific legislation or law for the control of cyber fraud so the

perpetrators knowing the facts are taking full advantage of this lacuna and targeting the financial sector as well as the individuals.

- The liability of service providers is very limited and they are taking advantage of the situation in present modern disputes. Service provider are protected under the blanket cover of law, if in situation of disputes between bank and the customer for the service of credit card in very situation service provider will always be saved and will not held liable because they are just a service provider and the issues of security of customer account details or their personal information than the bank will always liable
- There are lack of judgement and interpretation by the higher courts i.e., High Court and Supreme Court of India for cyber fraud cases. This has limited the development of law, regulation or statute for cyber fraud and this is explicitly creating a gap between the literatures.

**Suggestion:**

The research work has incorporated suggestions; some of the important suggestions are as follows

1. Law is silent on cyber fraud, there is no such law which has specifically dealt with cyber fraud. The Information and Technology Act must incorporate the definition of cyber fraud. The Information Technology Act (amendment Act 2008) both is silent on the issue of cyber fraud. Fraud committed on the bank is criminal in nature so the legislature considering all the relevant elements of fraud committed through the medium of technology must provide the definition so that

it can be convenient for the court to deal with such cases. Statute providing definition itself paved a easy way for the investigation and prosecuting authority. Without law and regulation, offenders of cyber fraud cannot be dealt in order to provide punishment.

2. Law is the only solution for cyber fraud. The Information and Technology Act, 2000 must incorporate cyber fraud so that it should shift their focus on the implementing process of cyber security considering all the people, process and technology. Banking or financial institutions must educate their employees regarding cyber security and the process of handling sensitive data, records, security technology such as authentic firewalls, genuine antivirus software, fraud detection tool etc. The Reserve Bank must strengthen Know Your Customer (KYC) norms. Another law that can be strengthened is that it is currently a civil offence under Indian Law, whereas it is a criminal offence in other countries. This needs to be reconsidered as per the demand of time.
3. Cyber fraud is computer fraud with involvement of technology in the absence of jurisdiction posing challenges making it difficult to conduct further investigation, including numerous jurisdictions and parties. Department needs to reframe the clauses to appoint the experts for the investigation process seeking proper forensic knowledge, information communication technology knowledge in order to prosecute their investigation plans. Investigating officer must be expertise in computer and forensic science. They must know how to handle the case of fraud occurring in cyberspace.

4. In most of the cases banks are found liable for the fraud that occurs in bank transactions or online unauthorized transactions. Banking staff have misused their position to temper with account holders card details for making unauthorized transactions. The Bank should take some strict measure for the requirement of the banking staff. Before appointing the staff they should be properly screened before they are employed and they must obtain satisfactory references. Banks should rotate the staff frequently so that they won't be able to obtain their personal gain.
5. Cyber fraud cases demand cooperative mechanisms that are not provided in the existing system which creates difficulties for the police to investigate crime outside Indian jurisdiction. Many cyber fraud offenders have evaded the prosecution due to the weakness in the existing law as that does not provide technological means of offences. However, how to amend the existing laws was not yet discussed.
6. India still needs to raise the bar of strong cybersecurity framework considering the combination of defence, resilience, and assurance mechanism. Government should ensure that their laws are absolutely applicable in order to combat cyber fraud. Even though enacted laws are inadequate, it's the individual responsibility to secure their information by using authenticated firewalls or by creating strong passwords. We must not forget that even laws are enforced in order to protect us or our rights; it will only work until and unless we ourselves take reasonable steps to protect our rights or property in the first place.

7. Even though RBI has been providing numerous guidelines for cybersecurity framework in banks which needs to be followed in an appropriate manner to combat cyber threats. The said security mechanism is not being properly followed by the banks. RBI has failed to provide policy in case of failure on the part of the bank to comply with guidelines provided by Reserve Bank of India.
8. Failure of the banks to train and appoint experienced staff having a background in subjects like computer systems are directly placed in such a position where there will be a need for knowledge about advanced technology. Bank authority need to set regular routing for the learning session about new technology, tactics, threats and new fraud which later on prove to be problematic for them to deal with.
9. For early detection of cyber fraud banks need to use the latest version of technology which can provide security. The bank should employ the best information technology system and data analytics in order to ensure effective implementation of the red flagged account (RFA) and get early warning signals (EWS) framework as suggested by Reserve bank of India, which helps in analyzing the patterns of transactions.
10. Internet banking provided more convenience to customers for managing their finance. Customers are advised not to reply more on mails, phone calls, or text messages asking about their personal information regarding their bank passwords, PIN numbers and OTP (one-time passwords), etc. We must keep in mind that banks never call, message, or mail you asking about your bank details.

11. Awareness can be a medium to fill the gap between banks and their customers. Banks must conduct more awareness programmes about cyber fraud mentioning different ways of fraudster targeting customers. Awareness can be done through email, ATM screens, social media, mobile applications, and even in public places with the help of banners and screens.
12. The Central Bureau of India (CBI) needs to conduct special training to Police and local enforcement officials in cyber cells and they much need to keep supervision for providing legal advice during the investigation.
13. India has enacted Information Technology Act, 2000 for regulating cyber law but there is lack of operational manual which describe detailed process and methods for conducting investigation. The Government of India needs to think about setting Standard Operating Procedure (SOP) for conducting investigation without any ambiguity.
14. India needs a proper standard procedure for seizure and analysis of digital evidence. In India there is insufficient funding for cyber crime, the law enforcement should look into this matter and there is a lack of trained cyber experts within law enforcement officials. Lesser numbers of cyber fraud before statutory are hampering effective enforcement of law. They need to allocate more resources for updating cybersecurity and provide regular training for cyber officials to impart highly specialized skills to combat cyber fraud. They must impart cyber crime courses in higher education such as in Law University in India.

15. Government and civil society should come together to work cooperatively in order to strengthen legal frameworks for cyber security. Jurisdiction creating issues must resolve with understanding, by creating agreements. There is always a lack of coordination for data sharing, which can be done by signing mutual agreements among the countries. India must define cyber fraud in a similar manner to other cyber crime. The Council of Europe Convention on Cybercrime addresses illegal access, computer related fraud, system interference and it encourages and assists to deal with these crimes. It also addresses investigation matters relating to jurisdiction and production and preservation of data. Basically the Convention on Cybercrime helps in promoting cooperation among the law enforcement officials' across national borders.
16. Information Technology Act, 2000 needs to incorporate the strict criteria for the liability of the service provider and they should be held liable for the negligence on the part of service they have provided.
17. The investigation of cyber fraud cases often involves the criminal justice system of different countries requiring international cooperation in order to bring perpetrators to justice. Multiple numbers of parties are involved so it was getting difficult to reach out the fraudster and to gather digital evidence. India needs more Multilateral treaties agreement which will make it easy to combat growing cybercrime. India must sign the Budapest Convention on cybercrime to combat cybercrime which is the only convention in international multilateral treaties dealing with cybercrime at the global level.

18. There is an urgent need for creating an umbrella law or convention which covers all major crimes related to cyberspace. Even specialized court in an international level as a sub-division court of the International Criminal Court should be established in order to deal with cyber issues. Indian legislators need to strengthen the domestic laws by bringing changes in order to claim over jurisdiction.
19. Jurisdiction issues have always left debatable, authorities are trying to overcome the jurisdiction restriction in national level by coordinating among the regionally. India should collaborate with other nations and create mutual Legal Assistants. To combat the challenges of cyber fraud as a new digital crime world need to come together and create Global Cyber Law. It would be easy to tackle cyber fraud without wasting time in the procedure for collecting electronic evidence which is causing delay in prosecuting the cases. Collaboration and rapid sharing of information are required between nations to combat the growing cyber fraud.
20. Now it's high time for Indian legislature to critically examine or evaluate the lacunas of the Information Technology Act, 2000 and amendment 2008. They should consider new digital technology crime or offence in order to secure the interest/ safety of the customer who from the time and again being victims of cyber fraud and judiciary are not able to give verdict in absence of specific section, law specifically dealing with the cyber fraud issues and punishment directly.



## REFERENCES

1. Aparna Viswanathan, “Cyber Law Indian & International Perspectives”, 2019, LexisNexis Butterworths Wadhwa Nagpur
2. Aastha Bhardwaj, Priyanka Gupta, “ IT Act 2000: Scope, Impact And Amendments”, International Journal of Electrical Electronics & Computer Science Engineering, ISSN: 2348-2273, 2015
3. B.R. Sharma, “Bank Frauds including Computer and Credit Cards Crimes Prevention and Detection”, 2<sup>nd</sup> Edition, Universal Law Publishing
4. Dr. R.K. Chaubey, “An Introduction to Cyber Crime and Cyber Law,” Published by Kamala Law house Kolkata, 2008 edition(2009 reprinted)
5. Justice Yatindra Singh, “Cyber Law”, 5<sup>th</sup> Ed, 2012, Universal Law Publishing Co. New Delhi-India at page 158, 169.
6. Karnika Seth, “Computers, Internet and New Technology Law”, 2<sup>nd</sup> Ed., LexisNexis at Page 56, 374.
7. Karnika Seth, “Computers, Internet and New Technology Law”, 2<sup>nd</sup> Ed., LexisNexis at Page 56, 374.
8. Dr. R. K. Chaubey, “An Introduction to Cyber Crime and Cyber Law”, Kamal Law House Kolkata
9. Dr. Talat Fatima, “Cyber Crime”, 2<sup>nd</sup> Ed, 2016, Eastern Book Company Lucknow at page 297 – 312, 317 – 321.
10. Nandan kamath, “Law Relating to Computer Internet & E-commerce”, 5<sup>th</sup> Ed, 2012 (Reprinted-2017), Universal Law Publishing LexisNexis at 18 – 25.
11. R. K Bangia, “ Indian Contract”, 6<sup>th</sup> Edition 2009, Allahabad Law Agency

12. National Cyber Crime Reference Handbook, Office of the Additional Director- General National Cyber Safety and Security Standards, Chennai, India, Vol. 11 .
13. Dr. Manju Koolwal, “White Collar Crime India &Abroad”, Kamal Publisher Delhi.
14. Aaron M. French, “*A Case Study on E-Banking Security- When Security Becomes Too Sophisticated for the User to Access Their Information*”, Journal of Internet Banking and Commerce, August 2012, vol. 17, no.2
15. Ahmad KabirUsman and Mahmood Hussain Shah, “*Critical Success Factors for Preventing e-Banking Fraud*”, Journal of Internet Banking and Commerce, Vol. 18 No.2, August 2013
16. A Simple Guide to Digital Evidence URL: Microsoft Word - digital.docx (forensicsciencesimplified.org)
17. A Simple Guide To Digital Evidence, URL: <http://www.forensicsciencesimplified.org/digital/DigitalEvidence.pdf> (visited on 22/2/2020)
18. Abdul RahamanKunji vs The State Of West Bengal on 14 November, 2014 (indiankanoon.org)
19. ATM Frauds in India evolved during Digitization URL: <https://indiaforensic.com/atmfraud.htm>
20. Arnaboldi Francesca and Claeys Peter, “*Internet Banking in Europe: a comparative analysis*”, Research Institute of Applied Economics 2008 URL: [http://www.ub.edu/irea/working\\_papers/2008/200811.pdf](http://www.ub.edu/irea/working_papers/2008/200811.pdf) (visited on 12.8.2018)

21. A committee headed by Shri S.R. Mittal was set up by RBI for Proposing Legislation on Electronic Fund Transfer and other Electronic. URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12_chapter%205.pdf)
22. Anubhav Pandey, " Indian Penal Code on Fraud and Cheating" URL: <https://blog.ipleaders.in/cheating-fraud/> (visited on 1/03/2019)
23. Anirudh Rastogi, " Cyber Law of Information Technology," 1<sup>st</sup> Edition 2014 Published by LexisNexis
24. Analysis Of Financial System Of RBI URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08_chapter%204.pdf) (visited on 5/8/2019)
25. Ashu Khanna & Bindu Arora, " A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry" Int. Journal of Business Science and Applied Management, Volume 4, Issue 3, 2009.
26. Association of Chief Police Officer (ACPO) of England define cybercrime <https://research.ijais.org/volume2/number2/ijais12-450261.pdf>
27. AP News dated: June 26, 2020 URL: <https://apnews.com/article/83ee48ae2a98aeb9a03a45df9e83eac3>
28. A Comparative Analysis of Customer Satisfaction in Nationalised and Private Banks in Madhya Pradesh 2001-2010" URL: <https://shodhganga.inflibnet.ac.in/bitstream/10603/114179/3/chapter-3.pdf> (visited on 4/8/2019)
29. Atay Erhan & Apak Sudi, " An overview of GDP and internet banking relations in the European Union versus China", Procedia- Social and

- Behavioral Sciences 2013 URL:  
<https://core.ac.uk/download/pdf/81163576.pdf> (visited on 10.2.2019)
30. Banking Law and Practice, 2014 URL:  
<https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20-Professional.pdf>
31. Banking Systems in India (Hilton- Young Commission) URL:  
<http://www.yourarticlelibrary.com/banking/reserve-bank/reserve-bank-of-indiaoriginand-development/26356>
32. Bank Frauds in India- An Analysis URL:  
<https://www.bankingfinance.in/bank-frauds-in-india-ananalysis.html>
33. B. Dutta & R.P Shukla, Banking Laws (Principles, Practice & Procedure), Dwivedi Law Agency, Allahabad, Volume.1 Edition. 2010
34. Bhasin. Dr. MadanLal, “*An Empirical Study of Frauds in the Banks*”, Vol. 4, No. 07, October 2015European Journal of Business and Social Sciences
35. Bindra P. S, “IT Implementation in Banking- Legal Implications”, September 30, 1999 URL: <https://rbi.org.in/scripts/PublicationsView.aspx?id=1572> (visited on 2/3/2019)
36. Black’s Law Dictionary 10<sup>th</sup> Edition also see FInal-Matter.pdf (cybertalkindia.com)
37. Brinda G. Lashkari, “Issue of Jurisdiction Under Cyber Law in India”, Racolb Legal (April 12, 2016), URL: <http://racolblegal.com/issue-of-jurisdiction-under-cyber-law-in-india/> (visited on 10/5/2020 )
38. CA Mayur Hoshi, Phishing in India is becoming innovative, URL: <https://indiaforensic.com/understanding-phishing-india/> (visited on 20/1/2020)

39. Cameron S. D. Brown, “Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice” *International Journal of Cyber Criminology* Vol 9 Issue 1 January – June 2015
40. Centeno Clara “Adoption of Internet Services in the Enlarged European Union: Lessons from Internet Banking case” June 2003, European Commission Joint Research Centre.
41. Chapter 2: E-Banking URL:  
<https://shodhganga.inflibnet.ac.in/bitstream/10603/89802/4/chapter%202.pdf>
42. Chibuko Raphael Ibekwe, *The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provision* (2015) Ph. D Thesis submitted to the School of Law, University of Stirling : URL:  
<https://dspace.stir.ac.uk/bitstream/1893/22786/1/Ibekwe%20PHD%20THESIS.pdf> (visited on 10. 09.2020)
43. Chand Smriti, “Reserve Bank of India: Origin and Development”, URL:  
<http://www.yourarticlelibrary.com/banking/reserve-bank/reserve-bank-of-india-origin-and-development/26356> (visited on 20/8/2019)
44. Clough Jonathan, “A World of Difference: The Budapest Convention on Cybercrime And The Challenges of Harmonisation”, URL:  
[https://web.archive.org/web/20160430024621/https://www.monash.edu/\\_\\_data/assets/pdf\\_file/0019/232525/clough.pdf](https://web.archive.org/web/20160430024621/https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf) (visited on 2/9/2018)
45. Customers’ Liability in Age of Digital Banking URL:  
<https://www.finextra.com/blogposting/14308/customer-liability-in-the-age-of-digital-banking>
46. Customer Protection for Limiting Liability of Customers in Unauthorized Electronic Banking Transaction (EBT) for the year 2018-2019 URL: policy-

for-customer-protection-for-limiting-liability-of-customers.pdf

(canarabank.com)

47. Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions URL: Reserve Bank of India - Index To RBI Circulars
48. Consumer Protection- Liability of Customers in Unauthorised Electronic Banking Transaction URL: Reserve Bank of India - Notifications (rbi.org.in)
49. “Committee on the Global Financial System: CGFS Papers No 60 Structural changes in banking after the crisis”, January 2018 URL: <https://www.bis.org/publ/cgfs60.pdf> (visited on 3/3/2019)
50. Cyber Space Jurisprudance URL: <http://assets.v mou.ac.in/PGDCL01.pdf>
51. Cyber Crime: Are The Law Outdated in India For This Type of Crime? URL: <http://www.legalserviceindia.com/legal/article-2454-cyber-crime-are-the-laws-outdated-in-india-for-this-type-of-crime-.html> (visited on 24/9/2020)
52. Cyber Crime Investigation Manual, Data Security Council of India, Delhi URL: [https://jhpolice.gov.in/sites/default/files/documentsreports/jhpolice\\_cyber\\_crime\\_investigation\\_manual.pdf](https://jhpolice.gov.in/sites/default/files/documentsreports/jhpolice_cyber_crime_investigation_manual.pdf)
53. Cyber Crime in India: Legislative And Judicial Response URL: [https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/12/12\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/12/12_chapter%204.pdf) (visited on 24/3/2020)
54. Dhupdale Vivek Y., “Cyber Crime and Challenges Ahead” March 2011 URL: [https://www.researchgate.net/publication/265166983\\_Cyber\\_Crime\\_and\\_Challenges\\_Ahead](https://www.researchgate.net/publication/265166983_Cyber_Crime_and_Challenges_Ahead) (visited on 10/5/2020)

55. Digital Evidence Law India and all Anvar v Basheer URL: Digital Evidence Law India (cyberblogindia.in)
56. Digital Evidence 2019 (March) URL: <https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html> (visited on 3/5/2019)
57. Digital Equipment Corp. v. Altavista Technology, Inc. 960 F. Supp. 456 (Decided on March 12, 1997) URL: Cybertelecom :: Internet
58. Dr. Farooq Ahmad, "Cyber Law in India Law on Internet", 4<sup>th</sup> Edition (2015) New Era Law Publications
59. Dr. Roshan Lal & Dr. Rajni Saluja, "E-Banking: The Indian Scenario", Asia Pacific Journal of Marketing & Management Review, Vol.1 (4), December (2012)
60. Dr. M. Imran Siddique, Sana Rehman, "Impact of Electronic crime in Indian Banking Sector – An Overview", International Journal of Business Information Technology, Vol. 1 No.2 September 2011.
61. Dr. Nidhi Saxena & Dr. Veer Mayank, "Forensic Hurdles in Investigation & Prosecuting Cyber-crime- An Overview", The Indian Police Journal
62. Dr. Roshan Lal & Dr. Rajni Saluja, "E-Banking: The Indian Scenario", Asian Pacific Journal of Marketing & Management Review, Vol. 1(4), December 2012 URL: <http://indianresearchjournals.com/pdf/APJMMR/2012/December/2.pdf>
63. Dr. Swapnil Sudhir Bangali & Dr. Harita Swapnil Bangali, In -Built Challenges for Information Technology Law in India, International Journal of Advanced Research (2016), Volume 4, Issue 6, URL:

[http://www.journalijar.com/uploads/973\\_IJAR-10800.pdf](http://www.journalijar.com/uploads/973_IJAR-10800.pdf) (visited on 5.6.2020)

64. Dr. Swarupa Dholam, *Electronic evidence and its challenges*, URL: [http://mja.gov.in/Site/Upload/GR/Title%20NO.129\(As%20Per%20Workshop%20List%20title%20no129%20pdf\).pdf](http://mja.gov.in/Site/Upload/GR/Title%20NO.129(As%20Per%20Workshop%20List%20title%20no129%20pdf).pdf)

65. Dr. VermaAmit and Bajaj Simi.k, “*Cyber Fraud: A Digital Crime*” 2008 [https://www.academia.edu/8353884/CYBER\\_FRAUD\\_A\\_DIGITAL\\_CRIME](https://www.academia.edu/8353884/CYBER_FRAUD_A_DIGITAL_CRIME)

66. Dr. S. Murugan, “Electronic Evidence: Collection, Preservation and Appreciation”, URL: [http://nja.gov.in/Concluded\\_Programmes/201819/P1125\\_PPTs/6.Electronic%20Evidence](http://nja.gov.in/Concluded_Programmes/201819/P1125_PPTs/6.Electronic%20Evidence)

67. Dr. Singh Tejinderpal, “*Security and Privacy Issues in E-Banking: An Empirical Study of Customers’ Perception*”, October 2013 URL: [http://www.iibf.org.in/documents/reseach-report/Tejinder\\_Final%20.pdf](http://www.iibf.org.in/documents/reseach-report/Tejinder_Final%20.pdf) (visited on 4/3/2019)

68. Dr. Hayes Ben, Dr. JeandesbozJulien, Dr. Ragazzi Francesco, Dr. Simon Stephanie & MitsilegasValsamis, “The Law enforcement challenges of cybercrime: are we really playing catch-up” , October 2015 URL: [https://www.researchgate.net/publication/283481769\\_The\\_law\\_enforcement\\_challenges\\_of\\_cybercrime\\_are\\_we\\_really\\_playing\\_catch-up](https://www.researchgate.net/publication/283481769_The_law_enforcement_challenges_of_cybercrime_are_we_really_playing_catch-up) (visited on 5/11/2019)

69. Dr. Jetling Yellosa, “Cyber Crimes and Legal Implications”, International Journal of Law, Vol. 2 Issue 2 (March 2016)

70. Douglas E-Commerce, *The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works* 4th Edition 2006.



71. DND India date: December 28, 2017 URL:  
<https://www.dnaindia.com/mumbai/report-2-romanians-held-in-delhifor-atm-fraud-in-mumbai-2571039>
72. DVA Public School v. The Senior Manager, India Bank, Midnapur Branch & Ors. CIVIL APPEAL NO. 9352 of 2019 URL:  
[https://main.sci.gov.in/supremecourt/2018/28537/28537\\_2018\\_8\\_1502\\_19253\\_Judgement\\_18-Dec-2019.pdf](https://main.sci.gov.in/supremecourt/2018/28537/28537_2018_8_1502_19253_Judgement_18-Dec-2019.pdf)
73. E-Banking, URL:  
<http://shodhganga.inflibnet.ac.in/bitstream/10603/89802/4/chapter%202.pdf>
74. Edwin Agwu & Mercy Agumadu, "*Analysis of the Emergent Issues in Internet Banking Adoption in Nigeris*", European Journal of Social Science, Vol. 52 No 2, June 2016 available at <http://www.europeanjournalofsocialsciences.com>
75. "Electronic Crime Scene Investigation: A Guide For First Responder", 2<sup>nd</sup> Edition, National Institute of Justice, April 2008
76. Ekaterina A. Drozdova, "Civil Liberties and Security in Cyberspace," Chap. 5 of this volume URL:  
[https://www.hoover.org/sites/default/files/uploads/documents/0817999825\\_183.pdf](https://www.hoover.org/sites/default/files/uploads/documents/0817999825_183.pdf) (visited on 9/12/2019)
77. Emerging Role as a Bankers' Bank URL: at  
<https://rbidocs.rbi.org.in/rdocs/content/PDFs/89639.pdf> (visited on 3/3/2019)
78. E. N. Roussakis. (1997), *Global banking: origins and evolution*. URL:  
<http://www.scielo.br/pdf/rae/v37n4/a06v37n4.pdf>
79. European Commission Report 2005 URL:  
[http://www.ub.edu/irea/working\\_papers/2008/200811.pdf](http://www.ub.edu/irea/working_papers/2008/200811.pdf) (visited on 10.8.2018)

80. European Central Bank: Structural Analysis of The EU Banking Sector  
November 2002 URL: <http://www.ecb.int> (visited in 10.9.2018)
81. Express News Service dated: September 17, 2018 URL:  
<https://indianexpress.com/article/cities/mumbai/vishing-case-retired-best-official-loses-lakh-claims-police-5359514/>
82. Framework for loan fraud URL:  
<https://home.kpmg/content/dam/kpmg/pdf/2015/06/Framework-Loan-fraud.pdf>
83. Financial Express dated August 20, November 2018 URL:  
<https://www.financialexpress.com/industry/banking-finance/how-rs-94-crore-online-fraud-was-carried-out-in-punes-cosmos-bank/1286068/>
84. Goel Dr. Pooja, “*Electronic Banking*”, University of Delhi URL:  
<https://sol.du.ac.in/mod/book/view.php?id=1225&chapterid=855> (visited on 5/3/2019)
85. Hamid Jahankhani, A. Al-Nermrat & Ami Hosseinian- Far, “Cyber Crime Classification and Characteristics,” November 2014, URL:  
[https://www.researchgate.net/publication/280488873\\_Cyber\\_crime\\_Classification\\_and\\_Characteristics](https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics) (visited on 21.1.2020)
86. History of Reserve Bank of India - GKToday also see URL:  
[https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/27702/8/08_chapter%204.pdf) (visited on 31/03/2020)
87. History of Online banking: How Internet Banking Went Mainstream by Ruth Sarreal, October 7, 2017 URL:  
<https://www.gobankingrates.com/banking/history-online-banking/>
88. Hosmer Chet, Proving the Integrity of Digital Evidence with the Time, International Journal of Digital Evidence Spring 2002 Vol.1, Issue 1 URL:

<https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf> (visited on 4.4.2020)

89. Indian Computer Emergency Response Team Ministry of Electronics and Information Technology Government of India, URL: <https://cert-in.org.in/>
90. India Today dated: September 10, 2020 URL: <https://www.indiatoday.in/crime/story/delhi-police-arrests-bank-agent-held-for-credit-card-fraud-1720662-2020-09-10>
91. India Today dated: September 10, 2020 URL: <https://www.indiatoday.in/india/story/fraudsters-steal-rs-6-lakh-from-ram-temple-trust-account-using-forged-cheques-1720533-2020-09-10>
92. India Today dated: September 10, 2020 URL: <https://www.indiatoday.in/crime/story/delhi-police-busts-cyber-fraud-nexus-having-roots-in-jamtara-jharkhand-1720307-2020-09-10>
93. India Today Dated: December 5, 2019 URL: <https://www.indiatoday.in/crime/story/indian-origin-man-jailed-cyber-fraud-uk-1625267-2019-12-05m>
94. India : Revisiting the Current Scenario of the Safeguards for Cybercrime URL: <https://www.lexology.com/library/detail.aspx?g=27a808e5-003d-4588-bbf1-c400a4c15b30> (visited on 10.8.2020)
95. The Indian Banking Sector: Recent Developments, Growth and Prospects” January 2013 URL: <https://www.ibef.org/download/Banking-Sector-04jan.pdf> (visited on 4/08/2019)
96. Investigating Cybercrime (2017), URL: [https://www.researchgate.net/publication/313164048\\_Investigating\\_Cybercrime](https://www.researchgate.net/publication/313164048_Investigating_Cybercrime) (visited on 14/1/2020) also see <https://cliffordodhiambo.wordpress.com>

97. International Cooperation in Cybercrime: The Budapest Convention URL:  
<https://cis-india.org/internet-governance/blog/vipul-kharbanda-april-29-2019-international-cooperation-in-cybercrime-the-budapest-convention> (visited on 25.5.2020)
98. The Times of India dated: September 4 URL:  
<https://timesofindia.indiatimes.com/city/delhi/delhi-gang-cheated-1000-credit-card-holders-in-2-years/articleshow/77923886.cms>
99. The Economic Times dated: 2<sup>nd</sup> January 2019 URL:  
<https://economictimes.indiatimes.com/industry/banking/finance/banking/watch-out-cyber-fraud-cases-in-banks-are-spiking/articleshow/6734975>
100. Jain Shubhra Jain, ATM Frauds- Detection & Prevention, International Journal of Advances in Electronics and Computer Science, Vol. 4, Issue- 10, October 2017 URL: [http://www.ijae.in/journal/journal\\_file/journal\\_pdf/12-410-151445396982-89.pdf](http://www.ijae.in/journal/journal_file/journal_pdf/12-410-151445396982-89.pdf) (visited on 23/7/2019)
101. 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 Practices, International Journal of Pure and Applied Mathematics, Volume 119 (2018) URL:  
<https://acadpubl.eu/hub/2018-119-17/2/135.pdf> (visited on 26.8.2019)
102. Joint Report Europol and Euro just Public Information June 2019 URL:  
[http://www.eurojust.europa.eu/doclibrary/Eurojustframework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20ombating%20cybercrime%20\(June%202019\)/201906\\_Join](http://www.eurojust.europa.eu/doclibrary/Eurojustframework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20ombating%20cybercrime%20(June%202019)/201906_Join)

tEurojustEuropolreport\_Common-challenges-in-combating-  
cybercrime\_EN.PDF

103. Jurisdiction URL:  
<http://14.139.60.114:8080/jspui/bitstream/123456789/742/9/Jurisdiction.pdf>  
(visited on 5/5/2020)
104. Kamble R.M & Vishwapriya C, “Cyber Crime And Information  
Technology”, NALSAR Law Review Vol-4 2008-2009
105. Kalra Kush, Emergence of Cyber Crime: A Challenge for the New  
Millennium, Bharati Law Review, April- June 2017 URL:  
[http://docs.manupatra.in/newsline/articles/Upload/4730150C-4A12-4EBA-  
8CAF-F1146FDD5657.pdf](http://docs.manupatra.in/newsline/articles/Upload/4730150C-4A12-4EBA-8CAF-F1146FDD5657.pdf) (visited on 27/8/2020)
106. Karishma Bhandari & Harvinder Soni, “*Indian Banking Sector: Then,  
Now & the Road Ahead*”, International Research Journal of Engineering and  
Technology (IRJET), Vol.3 Issue.4, April.2016
107. Kamau, Denis Mburu, “*Effects Of Technological Innovations On  
Financial Performance Of Commercial Banks In Kenya*” October 2013
108. Kaptan, S. S. (2003) *Indian banking in electronic era*. Sarup & Sons
109. Kumudha S & Rajan Aswathy, *A Critical Analysis of Cyber Phishing  
and its Impact on Banking Sector*, International Journal of Pure and Applied  
Mathematics, Volume 119 No.17 (2018) URL: [https://acadpubl.eu/hub/2018-  
119-17/2/128.pdf](https://acadpubl.eu/hub/2018-119-17/2/128.pdf)
110. K. Mani, *Electronic Banking Frauds [ATM, Mobile, Banking and  
Internet Banking]* published by Kamala Publishers, Edition 2016.

111. Law relating to cybercrime in India URL:  
[http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08\\_chapter%203.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08_chapter%203.pdf)
112. List of signatures and ratification of the Convention URL:  
<http://www.coe.int/en/web/conventions/full-list-/conventions/treaty/185/signatures> also see:  
[http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018\\_.pdf](http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018_.pdf) (visited on 29.8.2018)
113. L.S. Hoskote, “*Crime and Security in Electronic Banking*”, January 1996, CBI Bulletin Vol. IV
114. Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas, “*The Effects of Cyber Threats on Customer’s Behaviour in e-Banking Services*”, International Journal of e-Education, e-Business, e-Management and e-Learning Volume 7, Number 1, March 2017
115. Meaning, Concept and Classification of Cyber crimes URL:  
[https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11\\_cha%5bpter%203.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/188293/11/11_cha%5bpter%203.pdf) (visited on 1/2/2020)
116. Major Cyber Attacks on India (Exclusive New) dated 20th January 2020, URL: <https://www.testbytes.net/blog/cyber-attacks-on-india/> (visited on 2<sup>nd</sup> February 2020).
117. MacDonough v. Fallon McElligott, Inc. URL:  
[http://www.internetlibrary.com/cases/lib\\_case177.cfm](http://www.internetlibrary.com/cases/lib_case177.cfm)
118. Meijerink Tristan Janothan, “Carding Crime Prevention Analysis,” Politie Netherlands Police Agency, 2013 URL:

[https://essay.utwente.nl/63027/1/Understanding\\_processes\\_of\\_carding\\_versie\\_7\\_31-1\\_word.pdf](https://essay.utwente.nl/63027/1/Understanding_processes_of_carding_versie_7_31-1_word.pdf) (visited on 20.1.2020)

119. Maximum liability of a customer under paragraph 7 (ii) of RBI/2017-18/109 dated: 14, 2017 URL: [https://www.rbi.org.in/Scripts/BS\\_CircularIndexDisplay.aspx?Id=11188](https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11188)
120. Ministry of Communication and Information Technology National Cyber Security Policy, 2013, Department of Electronics and Information Technology URL: [https://nciipc.gov.in/documents/National\\_Cyber\\_Security\\_Policy-2013.pdf](https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf)
121. Mobile Banking transactions in India- Operative Guidelines for Banks URL: [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=1660](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1660)
122. Murlon- Druol Emmanuel, “*Banking Union in Historical Perspective: The Initiative of the European Commission in the 1960s-1970*”, Journal of Common Market Studies 2016 Vol.54 URL: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/jcms.12348> (visited on 27.9.2018)
123. Mumbai: Beware of E-wallet skimming, the trending cyber fraud URL: <https://www.dnaindia.com/mumbai/report-mumbai-beware-of-e-wallet-skimming-the-trending-cyber-fraud-2775826>
124. National Cyber Security Policy, 2013: Objectives URL: [https://nciipc.gov.in/documents/National\\_Cyber\\_Security\\_Policy-2013.pdf](https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf) (visited on 8.10.2020)
125. NASSCOM v. Ajay Sood and Ors 119 (2005) DLT 596, 2005 (30) PTC 437 Del URL: Success in any field of human activity leads to crime that need (delhicourts.nic.in)

126. Nidhi Arya, Cyber Crime Scenario in India and Judicial Response  
URL:  
[https://www.researchgate.net/publication/334124155\\_Cyber\\_Crime\\_Scenario\\_in\\_India\\_and\\_Judicial\\_Response](https://www.researchgate.net/publication/334124155_Cyber_Crime_Scenario_in_India_and_Judicial_Response)
127. NDTV Press Trust of India dated: July 10, 2020 URL:  
<https://www.ndtv.com/delhi-news/retired-delhi-university-professor-loses-rs-60-000-in-credit-card-points-fraud-cops-2260816>
128. News Special 18 dated 24<sup>th</sup> July 2017 URL:  
<https://www.news18.com/news/india/banking-frauds-who-is-responsible-bank-or-you-1471503.html>
129. Ostern Pvt. Ltd. &Anr v. State of West Bengal &Ors, AIR 2014 URL:  
<https://www.casemine.com/judgement/in/5ac5e3fa4a93261a672cfd6c>
130. Ompal, Tarun Pandey, Bashir Alam, “*How to Report Cyber Crimes in Indian Territory*”, International Journal of Science Technology and Management, Vol No. 6, April 2017
131. Online banking frauds: RBI says no loss to customer if fraudulent transaction reported in 3 days dated July 07, 2017 URL:  
<https://www.firstpost.com/business/online-banking-frauds-rbi-says-no-loss-to-customer-if-fraudulent-transaction-reported-in-3-days-3783491.html>
132. Pati Prathasarathi, Cyber Crime URL: CYBER CRIME (naavi.org)
133. Peretti Kimberly, “Data Breaches: What the Underground World of Carding Reveals,” Santa Clara High Technology Law Journal, Volume 25, Issue 2, 2009. URL: <https://core.ac.uk/download/pdf/149256649.pdf> (visited on 7.3. 2020)



134. Pretty Lather, *Cyber Crimes in India and the Legal Regime to Combat it*,” Dissertation (Unpublished) submitted to the Faculty of Law, University of Delhi, 2006
135. Poonia Dr. Ajeet Singh, *Cyber Crime: Challenges and its Classification*, International Journal of Emerging Trends & Technology in Computer Science Volume 2, Issue 6, November-December 2014 URL: <https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf> (visited on 21/8/2020)
136. Sarah Gordon, Richard Ford, “ On the definition and classification of cybercrime,” March 2006 URL: <http://index-of.es/Viruses/O/On%20the%20definition%20and%20classification%20of%20cybercrime.pdf>
137. Prepaid Payment Instrument (PPIs) URL: [https://m.rbi.org.in/scripts/FS\\_FAQs.aspx?Id=126&fn=9](https://m.rbi.org.in/scripts/FS_FAQs.aspx?Id=126&fn=9)
138. P.S. Lokhande, Dr. B.B. Meshram, “*Collecting Digital Evidence: Internet Banking Fraud - Case study*”, International Research Journal of Engineering and Technology (IRJET) Volume 2 Issue 2 May 2015
139. Puneet Mittal v. State Bank of India on 31 January 2015 URL: <https://indiankanoon.org/doc/159148066/>
140. Pyun, Chong Soo; Scruggs, Les; Nam, Kiseok, “ *Internet Banking in the U.S., Japan and Europe*”, Multinational Business Review, Fall 202 URL: <https://www.questia.com/read/1P3-146682121/internet-banking-in-the-u-s-japan-and-europe> (visited on 27.9.2019)

141. Ranka Shreyans, “All About E-contracts- Meaning, Types and Law”, 2015 available at <https://taxguru.in/corporate-law/all-about-e-contracts-meaning-types-and-law.html>
142. Raghavan A.R and ParthibanLatha, " The Effect of Cybercrime on a Bank's Finances," Vol.2 Feb 2014, International Journal of Current Research and Academic Review URL: <http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf>
143. Rattan Jyoti, Cyber Jurisdiction: A Seamy Side of Cyber Sovereignty With Special Reference To India (2018) 5 GNLU L. Rev. 52 URL: <https://www.scconline.com/Members/NoteView.aspx?enc=SIRYVC05MDAwMDY0NjcyJiYmJiY0MCYmJiYmU2VhcmNoJiYmJiZmdWxsc2NyZWVuJiYmJiZ0cnVlJiYmJiZjeWJlciBqdXJpc2RpY3Rpb24mJiYmJkFsbFdvcmRzJiYmJiZnU2VhcmNoJiYmJiZmYWxzZQ==> (visited on 5.8.2019)
144. RBI Guideline Vide Circular DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016
145. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017 dated: July 6, 2017 URL: <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11040>
146. RBI Vide Circular DBOD. AML. BC. No. 11/14.01.001/2012-13
147. RBI Notification on “Customer Protection- Limiting Liability of Customers of Co- operative Banks in Unauthorized Electronic Banking Transaction”, dated 14<sup>th</sup> December 2017 Reserve Bank of India - Index To RBI Circulars
148. Reserve Bank of India Functions.<https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20-Professional.pdf>

149. Reserve Bank of India Act, 1934 URL:  
[https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018\\_FCD40172EE58946BAA647A765DC942BD5.PDF](https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018_FCD40172EE58946BAA647A765DC942BD5.PDF)
150. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017 dated: July 6, 2017 URL: <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11040>
151. RBI Vide Circular DBOD. No. GC. BC. 193/ 17.04.001 dated November 18, 1993
152. RBI Notification dated November 05, 2015 URL:  
<https://rbi.org.in/Scripts/NotificationUser.aspx?Id=10111&Mode=0>
153. RBI Notification dated July 01, 2016 URL:  
<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD28A4C421E7F7724C07B38E3C6207F3548E.PDF>
154. RBI Master Circular :RBI/2015-16/1 dated: July 1, 2015 URL:  
[https://m.rbi.org.in/Scripts/BS\\_ViewMasCirculardetails.aspx?id=9808](https://m.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9808)
155. Reserve Bank of India Functions & Working Impacting Every Sector of The Economy & Touching Every Life Published by Dr. Rabi N Mishra, Chief General Manager and Principal, Reserve Bank Staff College, Chennai: November 2017 URL:  
[https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018\\_FCD40172EE58946BAA647A765DC942BD5.PDF](https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RWF15012018_FCD40172EE58946BAA647A765DC942BD5.PDF)
156. Reserve Bank of India: Functions and Workings URL:  
<https://rbidocs.rbi.org.in/rdocs/Content/PDFs/FUNCWWE080910.pdf> (visited on 2/8/19)
157. Rodrigue Glen Dario & Molina Fernando, “ The Preservation of Digital Evidence and Its Authority in the Court,” January 2017, URL:

- [https://www.researchgate.net/publication/312665626\\_The\\_preservation\\_of\\_digital\\_evidence\\_and\\_its\\_admissibility\\_in\\_the\\_court](https://www.researchgate.net/publication/312665626_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court) (visited on 28/4/ 2019)
158. Sanchi Agrawal, “*Cyber Crime in Banking Sector*”, Volume 3, May (2016)
159. Salaheddine J. Juneidi, “Council of Europe Convention on Cyber Crime”, 2002  
URL:[https://www.researchgate.net/publication/261363049\\_Council\\_of\\_Europe\\_Convention\\_on\\_Cyber\\_Crime](https://www.researchgate.net/publication/261363049_Council_of_Europe_Convention_on_Cyber_Crime)
160. Senior Branch Manager, United Bank of India v. Binoy Kumar Roy, Order dated 03-01-2017 URL:  
<https://www.casemine.com/judgement/in/5e1f03929fca19162beeba01>
161. Seema Goel, “*Cyber-Crime: A Growing Threat to Indian Banking Sector*”, International Journal of Science Technology and management Vol.No.5, Issue No.12, December 2016 available at  
<http://data.conferenceworld.in/IFUNA18DEC16/P13-20.pdf>
162. Shewangu Dzumira, “Electronic Fraud (Cyber Fraud) Risk In The Banking Industry, Zimbabwe”, Risk governance & control: financial markets & institutions / Volume 4, Issue 2, 2014
163. Seokhee Lee, Hyunsang Jun, Aangjin Lee, Jongin Lim, Digital evidence collection process integrity and memory information gathering, Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop Volume, Issue-7-9 November
164. Soni R R and Soni Neena, *An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks*, Vol. 2(7), 22-27, July (2013), Research Journal of Management Sciences.

165. Steven D. Hazelwood & Sarah Koon-Magnin, “*Cyber Stalking and Cyber Harassment Legislation in the United State: A Qualitative Analysis*,” Vol. 7 Issue 2 July 2013, International Journal of Cyber Criminology. URL: <https://www.cybercrimejournal.com/hazelwoodkoonmagninijcc2013vol7issue2.pdf>
166. Suneet Dwivedi, “Jurisdictional Issues in Cyber Crime”, available at [https://www.academia.edu/3700793/Jurisdictional\\_Issues\\_in\\_Cyber\\_Crime](https://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime)
167. Sukanya Kundu & Nagaraja Rao, “*Reasons Of Banking Fraud – A Case Of Indian Public Sector Banks*”, International Journal of Information Systems Management Research & Development (IJISMRD) Vol. 4, Issue 1, Jun 2014
168. Talib Mohammad & Sekgwathe Virginiah, “E-Crime: An Analytical Study And Possible Ways to Combat,” Vol. 2 May 2012, published by International Journal of Applied Information Systems URL: <https://research.ijais.org/volume2/number2/ijais12-450261.pdf>
169. Tejinderpal Singh, Security and Privacy Issues in E-Banking : An Empirical Study of Customers’ Perception Indian Institute of Banking and Finance (IIBF) October 2013 URL: [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=1660](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1660)
170. Talwant Singh, Cyber Law & Information Technology URL:<https://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf>
171. The European Banking Authority at a Glance URL: <https://eba.europa.eu/sites/default/documents/files/documents/10180/1401372/e8686db2-6390-4c52-ad06-bc8d24b7aeb5/EBA%20AT%20A%20GLANCE.pdf> visited on 13/6/2020

172. The Internet, URL: <https://ncert.nic.in/textbook/pdf/kect107.pdf>
173. The Times of India Gadgets News dated: September 10, 2020 URL:  
<https://timesofindia.indiatimes.com/gadgets-news/do-not-install-paytm-or-other-mobile-payments-app-from-unknown-links-govt/articleshow/78037607.cms>
174. The Hindu dated: February 26, 2020 URL:  
<https://www.thehindu.com/news/cities/chennai/delhi-based-vishing-gang-held-for-cheating-hundreds-in-tamil-nadu/article30917302.ece>
175. The Hindustan Times dated: 16 November 2019 URL:  
<https://www.hindustantimes.com/cities/15-months-later-no-lead-in-rs-94-cr-cosmos-bank-cyber-fraud-case/story-Ar6lk69HLJmBEyt9jGsx0K.html>
176. Traditional Functions of Reserve Bank of India URL:  
<https://accountlearning.com/traditional-functions-of-reserve-bank-of-india/>  
(visited on 6/08/2019)
177. “Touring the world of Cybersecurity Law”, San Francisco Conference 2016 URL:  
[https://www.rsaconference.com/writable/presentations/file\\_upload/law-w04-global\\_cybersecurity\\_laws\\_regulations\\_and\\_liability.pdf](https://www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf) (visited on 10/2/2019)
178. United States and European Union Approaches to Internet Jurisdiction and their Impact on E-commerce URL:  
<https://www.law.upenn.edu/journals/jil/articles/volume25/issue1/Chen25U.Pa.J.Int%27IEcon.L.423%282004%29.pdf> (visited on 21/5/2020)

179. Varun Tripathi, *Frauds and Cyber Frauds in Banking Sector* (2014) PL December 76 also see [https://www.rbi.org.in/scripts/BS\\_SpeechesView.aspx?Id=826](https://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826)
180. V. Gopal Krishna and G. Usha, *ATM Banking: Legal Issue of Security Concern*, ICFAI Journal of Banking Law, 2007
181. Verma Sandhya, “The Challenges of Cyber War A Critical Evaluation” (2017)  
URL:[https://shodhganga.inflibnet.ac.in/bitstream/10603/277965/10/10%20\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/277965/10/10%20_chapter%204.pdf) (visited on 13.2.2020)
182. Whitecomb Carrie Morgan, *An Historical Perspective of Digital Evidence: A Forensic Scientist’s View*, International Journal of Digital Evidence, Spring 2002 Vol. No. 1, Issue 1 URL: <https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf> (visited on 10.4.2020)
183. “What is Vishing? Voice Phishing Scams Explained & How to Prevent Them”, URL: <https://fraudwatchinternational.com/vishing/what-is-vishing/> (visited on 21.1.2020)
184. Why most cybercrimes in India don’t end in conviction. URL: <https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html> (visited on 10/8/2020)
185. Wu Yanbo, Xiang Dawei, Gao Jing Ming & Wu Yun, “*Research on Investigation and Evidence collection of Cybercrime Cases*”, 2018 IOP Con.Series: Journal of Physic: Conf. Series 117 (2019)

186. Yougal Joshi1 , Anand Singh, “*A Study on Cyber Crime and Security Scenario in India*”, International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013
187. Zarka Zahoor, MoinUd-din and Karuna, “*Challenges in Privacy and Security in Banking Sector and Related Countermeasures*”, International Journal of Computer Applications, Volume No 144 – No.3, June 2016
188. <https://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty>
189. [https://www.business-standard.com/article/pf/what-is-electronic-clearing-service-ecs-111070800019\\_1.html](https://www.business-standard.com/article/pf/what-is-electronic-clearing-service-ecs-111070800019_1.html) 20th January, 2013
190. <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0>
191. <https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20Professional.pdf>
192. <https://blog.ipleaders.in/cheating-fraud/>
193. <https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf>
194. [http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018\\_.pdf](http://ijless.kypublications.com/5.S2.18/IJLESS%205.S2-2018_.pdf)
195. [https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/148886/12/12_chapter%205.pdf)
196. Indian Express dated: March 32, 2020
197. <https://taxguru.in/corporate-law/all-about-e-contracts-meaning-types-and-law.html>
198. <https://www.icsi.edu/media/webmodules/publications/9.1%20Banking%20Law%20Professional.pdf>
199. <https://johnspaul7.blogspot.com/2019/03/st.html>



200. [http://nja.gov.in/Concluded\\_Programmes/2018-19/P-1125\\_PPTs/6.Electronic%20Evidence%20Collection%20Preservation%20and%20Appreciation.pdf](http://nja.gov.in/Concluded_Programmes/2018-19/P-1125_PPTs/6.Electronic%20Evidence%20Collection%20Preservation%20and%20Appreciation.pdf)
201. <https://eba.europa.eu/regulation-and-policy/single-rulebook>
202. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
203. [http://repository.out.ac.tz/987/1/Anipha\\_Mwingira.pdf](http://repository.out.ac.tz/987/1/Anipha_Mwingira.pdf)
204. <https://www.rbi.org.in/commonman/Upload/English/FAQs/PDFs/ECS140311.pdf>
205. <https://m.rbi.org.in/Scripts/FAQView.aspx?Id=63>
206. <https://eba.europa.eu/sites/default/documents/files/documents/10180/1401372/e8686db2-6390-4c52-ad06-bc8d24b7aeb5/EBA%20AT%20A%20GLANCE.pdf> (visited on 29.8.2018)
207. <https://www.ir.kiu.ac.ug/bitstream/20.500.12306/8947/1/img-0134.pdf>  
(visited on 16.05.2018)
208. [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf) (visited on 24.8.2018)
209. <http://legalserviceindia.com/legal/article-3210-cyber-crime-a-hindrance-in-digitalworld.html> (visited on 28.8.2018)
210. <https://www.slideshare.net/RanjanaAdhikari/cyber-crime-9203478>
211. <https://www.bajajfinserv.in/what-is-atm-fraud-and-types-of-atm-fraud>  
(visited on 20/1/2020)
212. The Times of India dated: September 23, 2020

213. <https://www.ndtv.com/india-news/atm-fraud-in-assam-4-foreigners-hack-atmsdupesbicustomers-of-crores-arrested-near-kolkata-police-2135234>  
Dated: November 19, 2019
214. <https://indianexpress.com/article/cities/mumbai/mumbai-cyber-fraudsters-dupe-78-year-old-of-rs-2-32-lakh-6638707>
215. <https://www.news18.com/news/india/banking-frauds-who-is-responsible-bank-or-you-1471503.html>
216. [https://www.naavi.org/cl\\_editorial\\_10/umashankar\\_judgement.pdf](https://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf)
217. <https://bnwjournal.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/>
218. <http://docs.manupatra.in/newsline/articles/Upload/4730150C-4A12-4EBA-8CAF-F1146FDD5657.pdf>
219. <https://www.ndtv.com/delhi-news/retired-delhi-university-professor-loses-rs-60-000-incredit-card-points-fraud-cops-2260816>
220. [https://www.livemint.com/technology/tech-news/govt-warns-of-serious-phishing-attack-starting-today-bewa re-of-this-email-id-11592718991047.html](https://www.livemint.com/technology/tech-news/govt-warns-of-serious-phishing-attack-starting-today-bewa-re-of-this-email-id-11592718991047.html)
221. <https://indiankanoon.org/doc/15001210/>
222. <https://www.casemine.com/judgement/in/59f95ced4a932658e9ccc2e5>
223. <https://www.news18.com/news/india/banking-frauds-who-is-responsible-bank-or-you-1471503.html>
224. The Times of India dated: November 21, 2020
225. The Indian Express dated: February 3, 2019
226. <https://rbidocs.rbi.org.in/rdocs/content/PDFs/89634.pdf> (visited on 5/06/2019)

227. <http://www.legalserviceindia.com/legal/article-3322-e-banking-frauds-and-indian-legal-prospective.html> (visited on 21.7.2020)
228. <https://www.ndtv.com/delhi-news/retired-delhi-university-professor-loses-rs-60-000-incredit-card-points-fraud-cops-2260816> (visited on 12.8.2020)
229. <http://www.cbi.gov.in/interpol/invletterrogatory.php> (visited on 15.6.2020)
230. <https://indiankanoon.org/doc/179788397/>
231. <https://indiankanoon.org/doc/781024/>
232. <http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf> (visited on 23/7/2019)