INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

LEGAL ASPECT OF ONLINE BANKING TRENDS IN INDIA

AUTHORED BY - DISHA KALRA

TABLE OF CASES

1. Akhilesh Kumar Singh v/s Bharti Airtel Limited & Another, First Appeal No. 403 of 2014
2. The Bank NSP Case
3. Mrs. Sucheta Charudutta Dhekane vs Bank of Maharashtra on 9 November 2011, CIC/SG/A/2011/002073
4. The PNB Scam, 2019

TABLE OF ABBREVIATIONS

1. E-banking	Electronic Banking
2. IT	Information technology
3. ATM	Automated Teller Machine
4. ECS	Electronic clearing system
5. NEFT	National Electronic Fund Transfer
6. RTGS	Real time gross settlement
7. CVV	Card verification value

 ISSN: 2582-6433

CHAPTER-01

INTRODUCTION

"Banks are the guardians of the savings of the people and perform an essential role in the development of a nation".

The banking structure of a country is very crucial for an economic system. It performs a significant role in the expansion and advancement of a nation's economy. The strength of a nation's financial system determines the nation's progress. The banking system is crucial because it gives individuals access to credit-based money. The banks serve as "financial intermediaries" between investors and savers, encouraging investment and the nation's economic growth. Additionally, banks provide individuals and organizations with a safe place to save their hard-earned money and the opportunity to earn interest on it.

These institutions also extend, banking services, to the poor and marginalised people hence aiding the financial inclusion and promoting inclusive growth.

Every industry in India has profited from the IT Revolution and economic reforms, including the banking sector. With the increased use of computer systems and the internet, there is a shift from conventional banking systems to internet-based banking systems, i.e., banks have shifted from "Brick to Click" [1]banking systems. Online banking, also known as electronic banking (e banking) or Internet banking, is viewed as a "value-added"[2] method of keeping and recruiting new customers while removing time-consuming and costly traditional banking services in the competitive financial system. The 'Internet' is presently being used as a platform to supply clients with an extensive variety of products and services.

Online baking, often known as internet baking, is the provision of traditional financial services to consumers over an online platform.

"*Internet banking, also known as Online banking, e- banking or virtual banking is an electronic payment system that enables the customer of the bank or other financial institutions to conduct a range of financial transactions through financial institutions website.*"[3]

[1] Uppal RK and Jha NK, Online Banking in India (Anmol Publications 2008)
[2] Supra note 1.
[3] Cashless India, (Oct 21, 2023) cashlessindia.gov.in

 ISSN: 2582-6433

"Online banking represents a new era in retail financial services. Customers can use online banking to get information and conduct financial transactions such as balance inquiries, inter account transfers, and bill payments, utility bill payment, cheque book request and so on, using a telephone network or otherwise without personally visiting the branches."[4]

1.1 FEATURES OF ONLINE BANKING

1. More secured way of banking
2. Hassel free process
3. Speedy process of performing banking transactions, as compared to traditional banking system.
4. Easy account management
5. Easy transfer of funds can be done, via, different modes like RTGS, NEFT, etc.
6. Provides 24* 7 banking services to the customers.
7. Online banking helps remove any kind of geographical barriers, as, the tractions can be done
   from 'Anywhere, Anytime'.
8. Internet is used as a platform, to perform, banking transactions.

1.2 ADVANTAGES OF ONLINE BANKING

The Advantages are as follows-

1. Unlike the Conventional financing system , the Online financing system is considered to be more convenient[5]. This form of banking can be done 24*7 from anywhere in the world, hence eliminating any form of geographical barriers. Almost all services which are available through traditional physical banks are available on the Online banking platform.
2. Online banking is 'Mobile' in nature ,i.e. it can be accessed anywhere in the world at any time , which is not available for physical banks.
3. The Online banking system perform quick and speedy transactions in real time. The funds can be sent both domestically and internationally through online banking system.
4. The depositor through online banking, can deposit and withdraw money from anywhere at any point of time from his bank account, at the time of need.

[4] Innovation in Banking sector- Challenges&Opportunities, research gate.net,(Oct 21 23.) www.researchgate.net
[5] Ibid note 1.

 ISSN: 2582-6433

1.3 DISADVANTAGES OF ONLINE BANKING

The disadvantages are as follows-

1. Online banking can only be performed when there is an Active internet connection. But, if there is constant disturbance, either due to power failures or Internet speed , it becomes difficult for a person to access the facilities of online based banking system.
2. Internet based banking, provides, services to customers on online platform, and , hence lacks personal interaction which can also be seen as a drawback.
3. Due to regular maintenance and upgradation of banking websites, new features get added in the banking website. This makes it difficult to operate for the tech-unsavvy and unaware customers.
4. Lack of trust in online banking between Banker and customer.

1.4 RISKS INVOLVED IN ONLINE BANKING

The online banking has bought revolutionary changes to the Indian banking sector. These changes are advantageous to both the Customers and banks. But, these changes have evolved new set of risks. Risks, are the expected or unexpected occurrence that may have an unfavourable consequence on the baking sector. Various risks associated with Internet banking, are:

1. When a bank initiates new products and services ,there is always a risk associated with it. The risk here lies in the future success and profits of such product or service. For declining such risks ,banks are supposed to conduct proper research and consult expert advisors in this field[6]. Also, the banks need to study their human resource, availability of capital etc.
2. When proper and timely online banking facilities are not performed by the banks it also can effect the repute of the bank. This can effect the banks ability to have new customers and to continue retaining the existing one's.
3. Online banking involves the risk of security. The security of banking institutions is harmed when any malicious person gets an unauthorised access on confidential information of the bank like the accounting systems. These form of activities, having a threat to the information security of banks can be done from anywhere in the world through any medium.

[6] Ibid note 1.

 ISSN: 2582-6433

4. Online banking involves 'Credit risk'[7]. This risk arises, when the money given by banks on credit basis to the customer aren't returned back to bank. Such form of risks arises when a customer fails to meet his credit obligation in a particular time frame.

1.5 FACTORS WHICH HINDER THE FINANCIAL INCLUSION OF MARGINALISED AND ILLITERATE PEOPLE IN ONLINE BANKING

1. **Lack of Access to Technology i**s one of the primary factor which hinders the financial inclusion of marginalised and illiterate people. These people generally have no, or, limited access to devices, which can hinder their access to online banking services.
2. **Limited digital literacy among the masse**s, is the second factor hindering the financial inclusion of the masses to online banking as to what is online banking, and how to use online banking.
3. **Limited knowledge and trust in technology** is also one of the factor hindering financial inclusion of marginalised and illiterate population. Due to limited trust in technology, the masses are afraid of frauds and maintaining security.
4. **Limited access to Internet and network connectivity** in areas, is also a hindering factor which hinders the financial inclusion of marginalised and illiterate population, and, hence they can't access online banking services.
5. These marginalised and illiterate population, **generally don't have necessary documents** required for accessing online banking services.

[7] Ibid note 1.

 ISSN: 2582-6433

CHAPTER-02

ONLINE BANKING TRENDS IN INDIA

The IT sector revolution has bought tremendous innovations in the banking institution of India. It has shifted the Indian banking system from "BRICK-CLICK"[8] system. Now, the banking functions can be performed at anytime, with, just a few clicks. Online banking has benefited both the bankers and the customers. These services can be accessed from anywhere in the world, hence, eliminates geographical barriers. It has facilitated banks, with, reduced transaction cost they can now offer more banking services to the customers.

In past, banks provided their clients with financial goods and services through conventional methods. But banks have now switched from conventional to online banking due to the internet, growing computer usage, globalisation, etc.

A few years ago, people thought banking was a simple industry. In the past, customers would deposit money into banks to get interest on it. They would be able to take money out of their accounts using cheques. However, banking is now done online via platforms. It is thought to be beneficial for banks as well as clients. With a few clicks and little effort, clients may now transfer money both locally and internationally.

2.1 WHAT IS ONLINE BANKING?

"Often E-banking is defined as a web based banking".[9]

Online banking, in the common sense, means to provide banking services over the internet platform. Other names for online banking include e-banking, internet banking, etc. By doing this, the banks are able to provide their customers with a greater selection of products and services at a lower cost per transaction. Customers can use these services online from the convenience of their own homes. Additionally, smaller banks may now compete on an equal basis with the biggest banks in the world thanks to internet banking.

Online banking can be seen as a service provided by the banks that allows the customer to perform various banking activities like checking account details, transfer of money, paying bills with just a few clicks.

[8] Ibid note 1.
[9] Hertzum elal.2004

 ISSN: 2582-6433

The term "e-banking" refers to "an electronic link between banks and customers for the purpose of organising and handling financial transactions."

Through the use of online banking, a person can connect through the banking website and perform various transaction. Various modes of online banking are Electronic funds transfer, ATM, Electronic clearing system (ECS) etc.

2.2 HISTORY OF ONLINE BANKING IN INDIA

Indian banking system has a long history. The past of Indian Banking system, can be classified into three stages:

1. Stage-1- Pre -Independence stage

In India, there were about 600 banks before to independence. In India's presidency towns, three banks were founded. The "Bank of Hindustan" in Calcutta was the nation's first bank, which, started to function in 1770. It carried on it's working until 1832. The "Bank of Calcutta" was founded in 1806. Later, in 1809, it changed its name to the" Bank of Bengal". "Bank of Bombay" and "Bank of Madra"s were established in 1840 and 1843 respectively. After the merger of the three banks in 1921, the "Imperial Bank of India" was formed. But as the country's central bank, the Imperial Bank of India was unable to fulfil its goals. Therefore, the Reserve Bank of

India was established based on the recommendations of the Hilton Young Commission.[10]

2. Stage-2 – Post Independence stage

The Government of India nationalised fourteen big private sector banks with deposits of at least 200 crores on July 19, 1969. These banks were nationalised in order to lend to farmers and small enterprises. fourteen banks, including the RBI, were nationalised in 1969. The British left India with big and minor privately owned banks, which were nationalised in the late 1960s, resulting in the establishment of public sector banks in India through the conversion of private to public sector banks.

The Government of India established many banking entities between 1982 and 1990 to give financial support to the needy, such as NABARD (1982) to provide aid for agricultural enterprises.

3. Stage -3 Economic Reforms

[10] Anwar, Saleem., Maharaja Sayajirao (2021), An Empirical Analysis of Agricultural Finance Provided by Scheduled Public and Private Sector Banks in India in the Post Reform Era (1991-2014)

 ISSN: 2582-6433

Until the 1990s economic changes, these banks operated under traditional banking structures. The 1990 banking reforms paved the door for establishing private sector banks and foreign banks in India. Following the introduction of the Internet and the widespread use of computer systems, private sector banks began using the Internet as a means to deliver financial services to its clients, paving the way for online banking in India. at 1996, the ICICI bank was the initial bank to 'provide online banking services' at its offices. 'This was followed by HDFC Bank, IndusInd Bank, and Citibank, in 1999, by, offering internet based banking services to it's customers'.[11]

2.3 TIMELINE OF ONLINE BANKING IN INDIA:

Timeline of online banking in India. In 1980-1990, debit and credit cards were introduced. Between 1984 and 1988, banks began to use 'computers, and MICR cheques were introduced'. HSBC was the first bank in India to introduce the ATM idea in 1987. The RBI launched ECS payments in India in 1990. India joined the Society for Worldwide Interbank Financial Telecommunication in 1991. in 1987. In 1997, a shared payment network system was established. In1999 The Reserve Bank of India, IIT (Mumbai), and IDRBT, Hyderabad collaborated on a smart card pilot project. The Information Technology Act was passed in 2000. SMS banking was the first kind of mobile banking in India in 2002. 'The launch of Special Electronic Fund Transfer. 2004 marks the introduction of real-time gross settlement in 2003.' In 2005, the Core banking systems were implemented in 11% of public sector bank branches, as well as national electronic funds transfer. 2008 - The introduction of a cheque truncation system and operational guidelines for mobile banking transactions. 2009 - ATM withdrawals are free.' In 2010 - The launch of an Immediate Payment Service'. In 2016, the Bharat Bill Payment System and the Unified Payments Interface were launched in banks across the country, with the first interfaces being uploaded in August 2016. [12]

2.4 TRENDS OF ONLINE BANKING BEFORE THE INFORMATION TECHNOLOGY ACT, 2000

1. ATM's

ATM, or 'Automated Teller Machine,' is a computerised device that allows clients to get financial services without the assistance of a bank personnel. A user can use an ATM to check his account balance, deposit money, withdraw cash and so on. These devices are

[11] Evolution of e-banking in India,(Oct 21, 2023) https://geniemoney.co.in/evolution-of-e-banking-in-india/
[12] Ibid note 4.

 ISSN: 2582-6433

user-friendly and simple to use. These may be used 24 hours a day, seven days a week. These machines are based on the concept of "Anytime-Anywhere" concept of banking[11]. To make use of an ATM, a person must have a debit or credit card and input a Personal Identification Number (PIN) to access ATM services. In 1987, HSBC was the initial bank in India to introduce the ATM idea. In 2009, free cash withdrawals from ATMs were permitted.

2. Debit Cards

Debit cards are plastic cards that may be used instead of cash for transactions. A debit card is a type of prepaid card. The vast majority of banks in India provide debit cards to its clients. It allows the customer to utilise ATMs and make online payments. If the consumer has a sufficient balance in his bank account, the money is automatically deducted. Debit and credit cards were introduced between 1980 and 1990.

3. Credit Cards

These plastic cards have a postpaid value. These cards essentially allow customers to buy products and services on credit and withdraw money from ATMs. Credit obtained by the client for any purchase or cash withdrawal from the bank must be refunded to the bank within a reasonable time limit and at a specified interest rate. Credit cards can be used to access ATM machines.

4. Electronic Clearing System (ECS)

Electronic clearing system, is a method of electronic fund transfer from one source to another. ECS system is generally used to make large and bulk transactions .ECS is used for the payment of EMI, pension, salaries etc. ECS system is used for making repetitive and regular transactions.

RBI, initiated ECS payment in India in the year 1990.

2.5 TRENDS OF ONLINE BANKING AFTER PASSING OF THE INFORMATION TECHNOLOGY ACT,2000

1. ***Mobile Banking***

This type of banking has further transformed India's internet banking system. This method allows users to complete banking operations with just a few touches on their mobile device. It essentially implies using a mobile device to execute banking activities. Mobile banking is often known as m- banking in common usage. Previously, m-banking was accomplished by text messages, but today mobile banking is accomplished through the installation of a bank application, which is accessible on both Android and iOS

 ISSN: 2582-6433

software. Customers may use the mobile banking application to transfer payments, check account balances, apply for loans and get cheque books, among other things. The primary distinction between Internet banking and mobile banking is that Internet banking is performed on computers, whereas mobile banking is performed on mobile devices. Mobile banking, was initiated in India by way of SMS banking, in 2002.

2. ***National electronic fund transfer(NEFT)***

   The NEFT service enables 'One to one bank transfer'. Under this system, money is exchanged via internet platform, rather then actual exchange of money through hands. It is basically a financial system wherein an amount is transferred from one person to another electronically. Herein, huge amount of money is involved , which makes it a risky transfer. Special Electronic fund transfer, was introduced in the year 2003.

3. ***RTGS***

   RTGS, or real-time gross settlement, refers to the transfer of payments on a 'order basis'. 'Real' refers to the processing of financial transfers in real time, that is, at that precise moment, rather than later. The term 'gross' refers to the settlement of monies. When a substantial volume of money is involved, RTGS is generally used. In 2004, real-time gross settlement was established.[13]

4. ***Cheque Truncation***

   Cheque Truncation is clearing of the cheques electronically, without the actual exchange of the cheques in a physical manner. The system of Cheque truncation was introduced in 2008 in India. The main aim behind this is, to increase the speed of cheque clearing system. It reduces the chances of misplacing the cheques, due to fault of bank employees.

5. ***Immediate Payment System(IPS)***

   Unlike RTGS and NEFT which are available only during the banking hours. The services of IPS is available 24 hours a day, 7 days a week.

   IPS provides ' real time inter banking transfers'[14] *clear tax. The banks customers can avail the facility of IPS through any device .IPS service, was introduced in 2010. The major participating parties for an IMPS transaction to take place are-*

   1.Remitter (Sender)

   2.Beneficiary (Receiver)

[13] Ibid note 1.

[14] Immediate Payment Service (IMPS) – What is IMPS Transfer, Timings, and Limit?, (Oct 21, 2023)cleartax.in

[14] Ibid note 1.

 ISSN: 2582-6433

3.Banks

4.National Financial Switch (NFS)[14]

Customers use the IMPS service to: Transfer funds, Receive payments and to Perform mobile banking transactions.

6. **UPI**

UPI, or Unified Payments Interface, is the most extensively utilised means of internet banking in India. In 2016, the National transfers Corporation of India (NPCI) launched it to encourage real-time monetary transfers. UPI enables customers to access and manage several bank accounts through a single site. Because each transaction requires a UPI PIN, this mode of transaction is entirely safe and secure. Transactions performed over UPI are normally free of charge. UPI 2.0, an updated version of the Unified Payments Interface (UPI), was released in 2018. Many features, such as overdraft capability, invoice creation on inbox, and so on, were added to expand UPI's capabilities. According to NPCI, 492 banks are participating in UPI as of September 2023, 492 banks are part of UPI system, with volume being Rs.10,555.69 million, and, value of Rs.15,79,133.18 crore[15].

7. **Artificial Intelligence and Chatbots**

Artificial intelligence is having a significant influence on the financial structure. The chatbots available on banks' websites assist in delivering 24*7 customer care to existing and new clients. These consumers may ask numerous bank related inquiries in the chatbots, which allows them to solve their problem at any time and from any location. Customers receive customer-specific recommendations for investments, loans, and so on.

CHAPTER -03

ONLINE BANKING: EFFECT ON CUSTOMERS AND BANKS

"I dream of a Digital India where mobile and e-Banking ensures Financial Inclusion."

[15] UPI Product Statistics, npci,org (Oct 20 2023) , www.npci.org.in

 ISSN: 2582-6433

PM Narendra Modi

Every element of human existence has been impacted by globalisation and the IT revolution, and the banking industry is no different. Only a small number of jobs in the banking industry were completed electronically in the past; the majority of work was done on paper. But, now in the present times, most of the business of banks is internet based, like ATM use, online banking, mobile banking etc., also referred as the "e-channels of banking".[16]. Private sector banks, foreign sector banks and some of the public sector banks provide online banking facilities to the customers.

Online banking has replaced traditional banking methods, resulting in a decrease in costs, paperwork, and time commitment. Consequently, there has been a rise in both customer satisfaction and bank productivity. Customers may use online banking services around-the clock. Customers and banks alike save money and time by using online banking. The internet banking system has helped banks become more productive and efficient. However, there are significant issues with security, trust, and other matters that the internet banking system has brought up for both banks and clients. Another name for electronic banking is electronic financial transfers.

3.1 EFFECT OF ONLINE BANKING ON BANKS

Online banking has restructured the Indian banking system. It has effected the Indian banking sector by providing positive effects to the banking sector, like, saving the cost, speedy banking etc., it has also posed certain negative effects and challenges to the banks.

3.1.1 POSITIVE EFFECTS OF ONLINE BANKING TO THE BANKS

1. The banks may **reduce transaction costs** by moving from expensive paper-based banking to internet banking. The banks' income rises as a result.
2. Online banking provides **Competitive advantage** to the banks.
3. Through online banking, the bank can reach the customers**, beyond geographical boundaries**, with a broad range of bank products and services to offer at a reduced cost.
4. Online banking **facilitates fast and speedy banking.** Through this the customer satisfaction is increased, as the transactions are done in a short span of time and the bank is able to manage more transactions in less time.

[16] Ibid note 1.

 ISSN: 2582-6433

5. This form of banking done by the banks on internet platform, is, both **time and cost effective.**
6. Banks, via, online banking can perform banking business without using paper money and by switching to plastic money, they can actually **save on production and storage cost of the paper currency.**
7. Banks may provide an **extensive variety of financial products and assistance to consumers via online banking,** which aids in acquiring new customers and maintaining existing ones.
8. 8.The Online based banking provides the customers, with, a **continuous 24*7 gateway to their accounts, which causes increased transaction and charges, resulting in additional revenue for the banks.**

3.1.2 NEGATIVE EFFECTS OF ONLINE BANKING TO THE BANKS

Online banking, with certain advantages also have certain disadvantages for the banks some of them are:

1. The banks, have to incur a **high commencement cost**, to, set up an online banking structure. Banks regularly incur such expenses, so as to maintain and upgrade the online bank services and platform.
2. Online banking involves, performing banking functions over internet. Banking functions include, depositing money, withdrawing money, transferring money etc. For this, the banks websites gather and save the customer's confidential account credentials. This makes online banking platform, **prone to "data breaches"** which can have legal and monetary results.
3. Technology keeps on evolving and changing. To meet with these changes, the banks also have to simultaneously and regularly keep updating and maintaining their online banking platforms to stand at a competitive advantage in the market. This process can be very **expensive** for the banks.
4. Due to online banking, there is no direct interaction between the banker personnel and customer. This lack of communication between the banker and customer, leads **to questioning of the reliability and credibility of bank by customer**, hence affecting the Banker-customer relationship.

3.2 CHALLENGES IN ONLINE BANKING TO BANKS

1. **Establishing and preserving customers faith** in online banking is very essential for

 ISSN: 2582-6433

the banks. For this, the banks need to maintain and regularly upgrade their online banking platform, for providing quality service to it's customers, and maintain the confidence of customers in bank. "Customer loyalty is a concern of any organizations as well as banking sectors."[17]

2. **Securely managing the confidential data of the customers**, on, online banking platforms is one of the challenges for the banks. For protecting customer's data from theft, hacking etc., the banks need have strict security policies
3. Due to various **operational factors**, the banks usually face various challenges like various technical and software glitches, system hang etc. which erodes customers confidence in the bank.
4. Banks have different categories of customers, including, young, old , tech-savvy, tech-unsavvy etc. For the old and tech- unsavvy customers, online banking becomes a difficult task. One challenge for the banks is to, **raise consumer awareness** as to how to use online banking.

3.3 EFFECT OF ONLINE BANKING ON CUSTOMERS

"The online banking service quality increases customer satisfaction because a banking customer can access various financial operations through online banking."[18] Online banking has a notable effect on the consumers. The customer, through online banking can, access banking 24*7, at any place, with just a few clicks. It is a convenient method of banking.

However, the customers face certain challenges, as to, cyberattacks, cyber theft, hacking etc.

3.3.1 POSITIVE EFFECTS OF ONLINE BANKING ON CONSUMERS

1. Through online banking, **the banking facility is available to the consumers, at their fingertips.** This facility can be used by the customers , 24 hours a day ,and, 7 days a week. This form of banking can be done from anywhere, hence, eliminating the geographical boundaries.
2. Unlike traditional form of banking, where the customers have to stand in long lines to perform their banking works done, online banking is **time saving and cost efficient**

[17] Alam- 2006
[18] Dhruba Kumar Gautam, Online Banking Service Practices and Its Impact on E-Customer Satisfaction and E-Customer Loyalty in Developing Country of South Asia-Nepal (Oct 21, 2023) journals.sagepub.com

 ISSN: 2582-6433

method of banking wherein the customer needn't go to bank, and, can through any device do banking work.

3. Through online banking, customers can make **quick and speedy transfer of funds,** from one source to another in just a short span of time. The transfer of funds can be done both domestically and internationally.
4. The customers also get the facility of **Online customer support** available on the bank's websites. These are specially designed chatbots, which can answer Frequently asked questions (FAQ's) of customers, at any time.
5. The services provided by banks, over, the online banking platform is **free of cost.**

3.3.2 NEGATIVE EFFECTS OF ONLINE BANKING ON CUSTOMERS

1. The prerequisite for accessing online banking is, internet. Without internet, a person can't access the banking functions. The customers access to online banking can be disrupted by**, unavailable and poor internet access.**
2. For performing banking functions, over the internet, a person has to enter his/her confidential bank account details on the server. These **details can be misused** by any person, who gains an unauthorised access to the server, resulting in legal and financial effects.
3. In online banking, the banks and the customers don't personally interact with each other, and hence there is **a lack of trust and confidence i**n banker- customer relationship.
4. Online banking, becomes very difficult to manage and operate for tech-unsavvy and senior citizens. With regular updates and maintenance in the banks websites, it becomes difficult to operate for people unaware of technologies.
5. Online banking is prone to various forms of cyberattacks, like, identity theft, hacking etc. These kinds of threats put the personal and privileged information of the consumers at a risk.

 ISSN: 2582-6433

CHAPTER-04

ONLINE BANKING AND CYBER CRIMES

In the Indian Penal Code of 1860 and the Information Technology Act of 2000, the terms "crime" and "cyber crimes" are not defined. These two Acts only stipulate the consequences of certain acts, such as cybercrimes. A reasonable definition of "crime" would be any unlawful act or omission that transgresses the law as it is now applied. The word "cyber" may conjure images of utilising the internet and computers. Consequently, any illegal activity involving the use of a computer is referred to as "cyber crime".

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as:

"*Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)*" [19]

The Council of Europe's cyber crime treaty, uses the term 'Cyber Crime' to refer to "*offences ranging from criminal infringement against data to content and copyright infringement*".[20]

The 'Computer' in cyber crime may be a facilitator or a medium to commit cyber crime, or, as a target of cyber crime.

"Douglas and Loader" have defined cyber crimes, "*as a computer mediated activity, which is conducted through global network, that are either considered as illegal or illicit by certain parties."*

"At the 'Tenth United Nations Congress on the Prevention of crime and treatment of offenders' cyber crime was categorised in two, and defined as-

a) *Cyber crime in narrow sense – Cyber crime is, any illegal act directed by means of electronic communications that target the security of the computer and information processed by them.*
b) *Cyber crime in broader sense- Cyber crime is an illegal act, which is committed by means of, or in, relation to a computer system or network, including such crimes as*

[19]Priya Pandey, CYBER CRIME AND ITS CLASSIFICATION, (Oct 21, 2023) https://www.scribd.com/document/380890531/08-chapter-2-1
[20] The Council of Europe's Cyber Crime treaty

 ISSN: 2582-6433

illegal possession and offering or distributing information by means of a computer system or network".[21]

The term "Cyber deception" refers to cybercrimes perpetrated in online banking, such as credit card information theft and infringements on intellectual property rights. India continues to rank fifth in the globe in terms of cybercrimes perpetrated internationally. Cybercrimes have risen in the banking industry as a result of increased computer system and internet usage. Both the banks and the clients suffer financial losses as a result of these kinds of offences.

4.1 CHARECTERISTICS OF CYBER CRIME-

a) Cyber crimes, have a global outreach, i.e., it can be committed by any person from anywhere in the world , by just , a few clicks. The attacker may be at one corner of the world, attacking, a victim, at another side of world.
b) Gaps in the software, often provide a chance to the attacker to get an unauthorised access in the computer system, and gain customer's personal information. These flaws in software, gives a chance to the attacker to take advantage of these gaps.
c) In cyber crimes, the attackers use an unidentified or a forged identity, so, that it becomes difficult to locate them. The attackers usually commit cyber crime, through an unknown, unidentified, or, pseudonyms name. The real identity is never disclosed by attacker.
d) Majority of the cyber crimes, are, committed by the attacker to gain financial benefit. Financial gain is the ultimate motive behind the commission of cyber crimes.

4.2 TYPES OF CYBER CRIMES

Generally, cyber crimes can be categorised into three kinds, depending on the target of crime. The types are-

4.2.1. Cyber Crime Committed Against An Individual-

Generally, an individual is the target of cyber crime. The reason behind this, is unawareness of the customers, in reference, to technology, lack of cyber- security and cyber safety measures. The various cyber crimes committed against individual

- **Cyberbullying**

Cyberbullying, has not been defined in the Indian law. It basically means, in layman's language, insulting , threatening someone through an electronic device. It includes,-

[21] Tenth United Nations Congress on the Prevention of crime and treatment of offenders

 ISSN: 2582-6433

- Embarrassing content posted on internet about the victim.
- Hacking someone's social networking accounts.
- Child pornography
- Threating, or, forcing a person to commit any illegal activity.

Section 67 of the IT Act,2000 punishes any *'person who transmits obscene material in electronic form*'[22]. It is the closest legal provision associated with cyber bullying. The punishment for such transmission is imprisonment for a term which may extend to five years and a fine which may extend to ten lakh rupees. [23]

Also, Section 66E of the IT Act states the punishment for 'violating any person's privacy through the internet'. Under this section, *any person who intentionally violates anyone's privacy by transmitting, capturing or publishing private pictures of others* shall be punished with imprisonment up to three years imprisonment or a fine of up to three lakhs.[22] Section 507 of IPC, also, provides that *any person who threatens anyone through anonymous communication* shall be punished with imprisonment for up to two years.[24]

- **Cyberstalking**

As the name suggests, cyberstalking is stalking someone , by, using computer sources and internet. The stalker usually stalks the victim by a spam identity, and are not easily traceable. It can be defined as a process, wherein the stalker stalks the personal accounts of the victim, browses victims online history and also sends obscene messages.

Section 67 of the IT Act states-

" ***Section 67****. Punishment for publishing or transmitting obscene material in electronic form- Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to*

[22] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)
[23] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India).
[24] The Indian Penal Code, 1860, Act 45, Act of Parliament

 ISSN: 2582-6433

five years and also with fine which may extend to ten lakh rupees".[25]

Section 354D of IPC, 1860 deals with stalking. It is somewhat related to cyberstalking as well.*" Under the Section, 354D. Stalking.--(1) Any man who—(i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or*

(ii) monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking:

Provided that such conduct shall not amount to stalking if the man who pursued it proves that-

(i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or

(ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

(iii) in the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine."[26]

Section 78. of The Bharatiya Nyaya Sanhita, 2023 (hereinafter referred as BNS, 2023) defines stalking as

"*(1) Any man who—*

(i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

(ii) monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking:

Provided that such conduct shall not amount to stalking if the man who pursued it proves that—

(i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or

[25] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)
[26] The Indian Penal Code, 1860, Act 45, Act of Parliament

 ISSN: 2582-6433

(ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

(iii) in the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine."[27]

- **Cyber Defamation-**

Cyber defamation is the damage of someone's reputation via the use of the internet. There are two sorts of defamation:

- Libel: It's a written defamatory comment. Writing libellous information, for example, is an example of cyber defamation in the form of libel.
- Slander: Any spoken defamatory comment that is published.

Section 67 of the IT Act, states the punishment for Cyber defamation i.e,

"Section 67. Punishment for publishing or transmitting obscene material in electronic form. Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees".[28]

• Phishing

Phishing is the deceitful practise of sending emails posing as legitimate organisations in order to persuade individuals to disclose personal and confidential data, such as passwords, credit card details, PINs, and so on, online. "The fraudulent practice of sending emails purporting to be from a reputable company in order to induce to reveal personal information, such as password and credit card information".[29]

[27] The Bharatiya Nyaya Sanhita, 2023, No. 45, Act of Parliament, 2023.
[28] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)
[29] Mrs. Sucheta Charudutta Dhekane vs Bank of Maharashtra on 9 November 2011

 ISSN: 2582-6433

Section 66C of the IT Act provides for punishment for phishing-related activities,

*" **66C Punishment for identity theft.** -Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh."*[30]

• Cyber Fraud

Cyber fraud refers to, "any act of fraud committed with the use of a computer." Any person who maliciously uses the internet to illegally cheat people and get access to personal data with an aim to make monetary gain is called a cyber fraud. There is no specific section stating punishment for cyber fraud.

But, **Section 420 of IPC,1860 which deals with cheating**, can be related to cyber fraud also. It states-

"Section *420. Cheating and dishonestly inducing delivery of property*.*—Whoever cheats and thereby dishonestly induces the person de-ceived 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.*"[31]

Section 318 (4) of BNS,2023 deals with Cheating-

"(4) 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."[32]

4.2.2. Cyber crime committed against an Organisation

• Data Diddling

[30] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)
[31] The Indian Penal Code, 1860, Act 45, Act of Parliament
[32] The Bharatiya Nyaya Sanhita, 2023, No. 45, Act of Parliament, 2023

 ISSN: 2582-6433

Data diddling is a cybercrime wherein there is a manipulation of data entries, without the permission of the owner, on a computer. It is generally committed by method of computer virus attacks.

In India, data diddling is punishable under Section 65 of the IT Act. The Section states

*"**Section 65. Tampering with computer source documents.***

Whoever knowingly or intentionally conceals, destroys 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 fine which may extend up to two lakh rupees, or with both.

Explanation.--For the purposes of this section, 'computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form".[33]

• Denial Of Service Attacks

Denial of Service (DoS) is a cyber attack on computer systems that prevents authorised users from utilising them. The attackers use deception to damage the targeted machine "until it ultimately crashes.

Section 66F of the IT Act, deals with cyber terrorism. As per the said Section,

"***Section 66F. Punishment for cyber terrorism.***

(1) Whoever,--

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage

[33] Ibid note 30.

 ISSN: 2582-6433

or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise ,commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life."[34]

4.2.3. Cyber crime committed against the society at large

• Cyber Terrorism

Cyber terrorism means using internet and computer systems, to cause damage the general public and 'damage the integrity and sovereignty of the country.'

The IT Act defines cyber terrorism under Section 66F as any

"*Section 66F. Punishment for cyber terrorism.*

(1) Whoever,--

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect

[34] Ibid note 30.

 ISSN: 2582-6433

the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life."[35]

• Cyber Pornography

Pornography is defined as "the depiction of erotic behaviour (as in pictures or writing) intended to cause sexual excitement." Thus, cyber pornography is defined as "the use of the internet to display, distribute, import, or publish pornography or obscene materials.

Section 67 of the IT Act, states cyber pornography. It states that,

"***Section 67. Punishment for publishing or transmitting obscene material in electronic form.*** *Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees*".[36]

4.3 TYPES OF CYBER CRIMES IN ONLINE BANKING

1. HACKING

Basically, hacking can be defined as an act to gain an unauthorised access into someone else's

[35] Ibid note 30.

[36] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)

 ISSN: 2582-6433

computer system. The Information Technology Act,2000 doesn't define the term 'Hacking'. But, by the conjoint reading of Section 43(a) of The IT Act, 2000, Section 66 of The IT (Amendment)Act, 2008 and Section 379 and 406, a hacker can be sentenced. Before The IT(Amendment) Act, 2008, Section 66 only prescribed a punishment extendable up to 3 years, or. fine extendable to Rs. 2 lakh. *After coming up of The IT (Amendment)Act, 2008, the amount of fine that can be imposed has increased from Rs 2 lakhs* to Rs. 5 lakhs. Now, hacking is considered to be Cognizable offence.

2. CREDIT CARD RELATED OFFENCES

Credit card offences often occur when an unauthorised person obtains access to the victim's credit card. The preparator can take money out of the victim's bank account and use the credit card to make illegal purchases of goods and services under the victim's identity. One may suffer financial losses as a result of this. When a victim electronically inputs his credit card information on a dubious website, credit card information is typically obtained by the person planning the crime.

3. KEYLOGGING

Another name for it is keystroke logging. As the name implies, the individuals responsible for this cybercrime actually track every mouse click and keystroke a user makes on his own computer. These apps are essentially "Trojan software programmes" that are installed on the computer. These infections are quite dangerous to people since they have the ability to capture all of a person's private and sensitive information, including bank account information.

4. VIRUSES

Viruses are the programmes which effect the functioning of the computer system. Due to the presence of viruses, the computer system can function in an absurd manner. The presence of virus, in computer system can pose a great risk to computer system. Yet, another form of programmes is Worms. They replicate themselves in the computer system. They don't change or remove any files from computer. They only multiply and send confidential information from victims computer to Hacker's computer.

5. SPYWARE

It is also one of the cyber crime which effects online banking in India. As the name suggests, these programmes spy, i.e., it basically records the information on computer system, or, the information which is transmitted from one computer system to another. It usually appears on

 ISSN: 2582-6433

different websites in the form of "pop- up ads" asking the user to install unscrupulous software's. These software's if installed on computer system, can harm the privacy and security of a person's account, and, make it unsafe for the person to perform online banking functions on system.

6. MALWARE OFFENCES

It is considered to be one of the most common threat to the Indian banking system. Herein, a fraudulent code is framed. This fraudulent code in computer system can infringe the computer system security. This can also effect the online banking functions performed on computer system. The number of malware attacks are increasing in the banking industry.

7. PHARMING

It is among the most frequent cybercrimes in the financial industry. It is easy to trick customers with pharming. In pharmacy, the client uses the computer system's URL to log in to the banks' websites. The bank's URL is accessed unauthorisedly by the criminals who are planning the crime. After that, the user is sent to a fictitious bank website that impersonates the actual but isn't. Here, the victim is easily tricked since the criminals develop a website that is virtually a copy of the genuine bank website. It gets harder to tell the two websites apart since they are so similar to one another.

8. ATM SKIMMING

Point of sale crimes are another name for these offences. Here, "skimming device" is placed on the device card reader or the ATM keypad. The way the skimming device is mounted gives the impression that it is a component of the ATM. The preparator behind ATM skimming wants to get the cardholder's personal identification number (PIN), card number, expiration date, and CVV. The preparator uses these data to get unlawful access to the users' bank accounts.

4.4 EFFECTS OF CYBER CRIMES ON ONLINE BANKING

Cyber crimes have become a growing threat to the online banking sector in India. With the growing use of computer systems and internet, cyber crimes have tremendously increased, in the Indian banking sector. These crimes effect the individual and also the economy at large. The various effects of cyber crimes on online banking are:

1. Cyber crimes committed in online banking**, infringes, the privacy of the customers**. Through cyber crimes, any person from any corner of world, can

 ISSN: 2582-6433

infringe the privacy of person at another corner of world, by, getting a fraudulent access to other person's account.

2. Cyber crimes committed on online banking platform can lead to **reputation loss** for both the banks, and, the customers.
3. It can lead to **financial loss to the customers.** The preparators through cyber crimes, can access the bank accounts and confidential information of the victim, causing financial loss to victim.
4. Through cyber crimes committed in online banking, the banks and the customers may have to **face legal consequences.**
5. Cyber crimes committed by preparators, can lead to **infringement of trust and confidence,** by the customers on banks.

4.5 CASE- THE BANK NSP CASE

The facts of this case were, that, a person who was the 'management trainee' of a bank was to get married. The couple used to exchange a lot of e-mails, through, the bank's computer system. When the couple got separated, the girl created various fraudulent email id's like 'Indian Bar Association' etc, and sent money to the person's clients. All these mails were sent by the girl, through the bank's computer system. Due to such mails, the bank suffered losses. The clients took bank to the court, wherein the bank were held liable for the mails sent.[37]

4.6 PREVENTION STEP GUIDE

To prevent cyber crimes, the following prevention tips can be followed-

1. There is a need to create awareness among the people, and, especially in children who have the curiosity of using internet and free access of internet and computer system, become thee common victims of banking frauds.
2. The customers should create a difficult to guess password. The password should be regularly changed.
3. The customers should use Two- factor Authentication, to add an additional layer of security to the banks account. Through this authentication, a person can avoid any fraudulent access in the person's account.
4. The customers should use, Secured networks to perform banking transactions.
5. The banks should also employ 'verification methods' to perform banking transactions.

[37] Ibid note 1.

 ISSN: 2582-6433

CHAPTER-05

LEGAL ASPECTS OF ONLINE BANKING IN INDIA

The banking system is the backbone of a nation's economic structure. The future anticipated growth of a country's economy depends on how strong the banking structure of an economy is. The business of collecting deposits from the general public for the purpose of lending, or

 ISSN: 2582-6433

financing, returning money upon request, and allowing money to be withdrawn through financial instrument is known as banking. Internet can be said as 'Information Superhighway'[38], as it has the capacity to connect innumerable people together on same platform.

The introduction of Information technology in banking, has bought the banking structure of India one step ahead. The introduction of IT revolution in the Indian banking sector has shifted the structure of the Indian banking from "Brick-to- click"[41] banking structure. With the introduction of Internet, and the popularisation of the computer systems, the banks are now increasingly using internet, as a platform, to provide a range of products and services to it's customers, at a reduced transactional cost. In simple terms, online banking can be described as performing traditional banking functions, online. The process of e-banking is a dynamic and a transitional process.

5.1 LEGAL FRAMEWORK OF ONLINE BANKING IN INDIA

Online banking, isn't a separate business done by banks. It is the same traditional business done by banks, but, on the online platform. Banking in India is governed by various laws and statutes, like, The Banking Regulation Act, 1949, The Information Technology Act, 2000 (hereinafter ITAct,2000), 'The Reserve Bank of India Act,1934 '(hereinafter RBI Act,1934), The Indian Penal Code,1860 (hereinafter IPC,1860) ,Consumer Protection Act,2019 and Internet banking guidelines issued by RBI .

5.2 LAWS BEFORE THE INFORMATION TECHNOLOGY ACT,2000 ON ONLINE BANKING

1.THE BANKING REGULATION ACT,1949

The preamble to the Act, states, the objective of the framing of Act, i.e.,

"*An Act to consolidate and amend the law relating to banking, WHEREAS it is expedient to consolidate and amend the law relating to banking."*

a. Section 35A. Power of the Reserve Bank to give directions.-

"(1) Where the Reserve Bank is satisfied that--

(a) in the public interest; or

(aa) in the interest of banking policy; or to prevent the affairs of any banking company being

[38] Volume 2, Bhagtan Gunjan & Pandya Jhanvi, Contemporary Legal Issues in Indian E Banking System, ,2019 [41] Ibid.

 ISSN: 2582-6433

conducted in a manner detrimental to the interests of the depositors or in a manner prejudicial to the interests of the banking company; or

(b)*to secure the proper management of any banking company generally,*

it is necessary to issue directions to banking companies generally or to any banking company in particular, it may, from time to time, issue such directions as it deems fit, and the banking companies or the banking company, as the case may be, shall be bound to comply with such directions.

(2) The Reserve Bank may, on representation made to it or on its own motion, modify or cancel any direction issued under sub-section (1), and in so modifying or cancelling any direction may impose such conditions as it thinks fit, subject to which the modification or cancellation shall have effect".[39]

Section 35 A gives power to Reserve Bank of India, to issue directions to the banking companies, when RBI is satisfied that there is public interest, or to secure the proper management of any banking company. It isn't specifically related to online banking, but it gives power to RBI to issue directions to banks regarding online banking.

2. THE INDIAN PENAL CODE,1860 AND THE BHARATIYA NYAYA SANHITA, 2023

Many online banking crimes, are punishable under the Indian penal code,1860. These are-

a. *Section 378 and Section 379 of IPC, 1860: Theft and punishment for theft*

Section 378 of IPC,1860 describes theft. Theft, also includes 'Data theft' also. Data protection is important. The data can be stolen from the computer system, through various means, like Hacking, Denial of service, spreading of viruses and worms etc. Section 379 IPC,1860 prescribes punishment for theft, and states that anyone, who tries to 'steal any movable property' which also can be an 'electronic record' can be punished with *imprisonment which may extend to three years or with a fine or both.*[40]

Section 303(1) and (2) of BNS, 2023; Theft and Punishment for theft

"303*. (1) Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.*

Explanation 1.—A thing so long as it is attached to the earth, not being movable property,

[39] The Banking Regulation Act,1949, No.10., Act of Parliament, 1949(India).

[40] The Indian Penal Code, 1860, Act 45, Act of Parliament

 ISSN: 2582-6433

is not the subject of theft; but it becomes capable of being the subject of theft as soon as it is severed from the earth.

Explanation 2.—A moving effected by the same act which affects the severance may be a theft.

Explanation 3.—A person is said to cause a thing to move by removing an obstacle which prevented it from moving or by separating it from any other thing, as well as by actually moving it.

Explanation 4.—A person, who by any means causes an animal to move, is said to move that animal, and to move everything which, in consequence of the motion so caused, is moved by that animal.

Explanation 5.—The consent mentioned in this section may be express or implied, and may be given either by the person in possession or by any person having for that purpose authority either express or implied."[41]

b. *Section 419 IPC: Cheating by Personation*

Section 419 of IPC states punishment for any act committed through cheating by personation, i.e. *," imprisonment of either description for a term which may extend to three years, or with fine, or with both."*[44] Section 66-C of IT Act also provide punishment for the same, i.e. *," imprisonment of either description for a term which may extend to three years, or with fine, or with both*".[42] Any person who commits the offence of cheating by means of computer is said to do Cheating by Personation.

Section 319(2) of BNS,2023 states Cheating by Personation-

"(2) Whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both."[43]

c. *Section 499 IPC: Defamation*

"*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm ,or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that*

[41] The Bharatiya Nyaya Sanhita, 2023, No. 45, Act of Parliament, 2023.
[42] Supra note. 40.
[43] The Bharatiya Nyaya Sanhita, 2023, No. 45, Act of Parliament, 2023.

 ISSN: 2582-6433

person.

Explanation 1.—It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Explanation 2.—It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Explanation 3.—An imputation in the form of an alternative or expressed ironically, may amount to defamation.

Explanation 4.—No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a lothsome state, or in a state generally considered as disgraceful."[44]

According to Section 500 IPC, the punishment for defamation is imprisonment which may extend to two years or fine or with both.'

Section 356(1) of BNS,2023 states Defamation as

"356. (1) Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes in any manner, any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.

Explanation 1.—It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Explanation 2.—It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Explanation 3.—An imputation in the form of an alternative or expressed ironically, may amount to defamation.

Explanation 4.—No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual

[44] The Indian Penal Code, 1860, Act 45, Act of Parliament.

 ISSN: 2582-6433

character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.[45]

3.THE NEGOTIABLE INSTRUMENTS ACT,1881

The preamble to the Act states , "*An Act to define and amend the law relating to Promissory Notes, Bills of Exchange and Cheques.*"[46]

There is only one provision relating to Online banking in India, i.e., Section 6-

a. Section 6 Cheque

"*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.*

Explanation I.-- For the purposes of this section, the expressions

(a) a cheque in the electronic form means a cheque drawn in electronic form by using any computer resource and signed in a secure system with digital signature (with or without biometrics signature) and asymmetric crypto system or with electronic signature, as the case may be;

(b) a truncated cheque means a cheque which is truncated during the course of a clearing cycle, either by the clearing house or by the bank whether paying or receiving payment, immediately on generation of an electronic image for transmission, substituting the further physical movement of the cheque in writing.

Explanation II. -- For the purposes of this section, the expression clearing house means the clearing house managed by the 'Reserve Bank of India 'or a clearing house recognised as such by the 'Reserve Bank of India'.

[Explanation III. -- For the purposes of this section, the expressions asymmetric crypto system, computer resource, digital signature, electronic form and electronic signature shall have the same meanings respectively assigned to them in the Information Technology Act, 2000 (21 of 2000)".[47]

Section 6 of The Negotiable Instruments Act, 1881 defines a Cheque. It states, that 'cheque is a bill of exchange drawn on a specified banker'. It includes the electronic image of a truncated cheque.

[45] The Bharatiya Nyaya Sanhita, 2023, No. 45, Act of Parliament, 2023.
[46] The Negotiable Instruments Act,1881, No. 26, Act of Parliament,1881(India).
[47] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India

 ISSN: 2582-6433

5.3 LAWS AFER THE INFORMATION TECHOLOGY ACT, 2000 ON ONLINE BANKING

1.THE INFORMATION TECHNOLOGY ACT, 2000

The main law pertaining to e-commerce is the Information Technology Act, 2000 (henceforth referred to as the IT Act, 2000). The Reserve Bank of India Act, 1934 and The Banking Regulation Act, 1949 serve as the primary laws governing internet banking in India; however, the IT Act, 2000 regulates all online offences.

Preamble of The IT Act,2000 states that-

"*An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books, Evidence Act, 1891 and the' Reserve Bank of India Act, 1934 'and for matters connected therewith or incidental thereto".*[48]

Various sections dealing with Online banking are-

a. Section 43.Penalty for damage to computer, computer system, etc.

"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 secures 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;

[48] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)

 ISSN: 2582-6433

(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."[49]

According to Section 43 of The IT Act, 2000 if any person**, without consent of the owner, gets an unauthorised access in the computer system of a person** , gains accesses or secures access to such computer , or, **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; **Or introduces or causes to be introduced any computer contaminant or computer virus into any computer,** computer system or computer network; 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**; disrupts or causes disruption of any computer, computer system** or computer network; **denies or causes the denial of access to any person authorised to access any computer,** computer system or computer network by any means; 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**; 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,**

then that person shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

b. Section 43A. 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 and maintaining reasonable security practices and procedures and thereby*

[49] Ibid note 48.

 ISSN: 2582-6433

causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected".[50]

When any body corporate, which handles any sensitive and confidential information, is negligent in maintaining security standards, and, causes wrongful gain or wrongful loss to a person , then, such body corporate shall be liable to pay damages by way of compensation to the person affected. This provision has been added by The Information Technology (Amendment) Act, 2008.

c. Section 66.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*."[51]

According to Section 66 of the Act, if any person without the consent of the owner, gets an unauthorised access to a persons computer system, or, the preparator of the crime performs any of the act as specified in Section 43 of the Act, the preparator shall be punished with, imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both."

d. Section 66C Punishment for identity theft.

"*Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh".*[52]

According to a common sense definition, identity theft is the theft of a person's personal identity and use of it by another person for illegal or dishonest purposes. According to Section 66C of The IT Act, 2000, there is a three-year maximum sentence for any individual found guilty of using another person's electronic signature, password, or other unique identifying feature fraudulently. In addition, there is a potential fine of one lakh rupees. The Information Technology (Amendment) Act of 2008 included this clause.

e. Section 66D Punishment for cheating by personation by using computer resource.

[50] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)
[51] The Information Technology Act, 2000, No. 21, Act of Parliament,2000 (India)
[52] Ibid note 50.

 ISSN: 2582-6433

"*Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees".*[53]

"Impersonation" is the act of someone pretending to be someone else in order to obtain an unfair advantage. The IT Act's Section 66D penalises "personation" that occurs online, or over an internet connection. As to the provisions of Section 66D, any anyone who uses a computer device to commit personation faces the possibility of imprisonment for up to three years, as well as a fine of up to one lakh rupees. The Information Technology (Amendment) Act of 2008 included this clause.

f. Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.-

"(1) *Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.*

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to—

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b)intercept, monitor, or decrypt the information, as the case may be; or

(c) *provide information stored in computer resource.*

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to

[53] Ibid note 50.

 ISSN: 2582-6433

seven years and shall also be liable to fine".[54]

Section 69 of The IT Act,2000 empowers the Central Government or a State Government to intercept, monitor, or decrypt the information in any computer system. Sub- section 3 of Section 69 of the Act, states that if the subscriber or intermediary fails to assist the agency shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

g. Section 72A. Punishment for disclosure of information in breach of lawful contract

"*Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both."*[55]

Section 72A of IT Act,2000 provides for 'punishment for disclosure of information in breach of lawful contract'. This section states that, if any person, including an intermediary if gets an access to personal information of a person, and with an intent to cause wrongful gain or loss to another person, discloses without the consent of the owner, such material information 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." This provision has been added by The Information Technology (Amendment) Act, 2008.

h. <u>Section 85 Offences by companies</u> "(1*) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.*

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the

[54] Ibid note.50.
[55] Ibid note 50.

 ISSN: 2582-6433

provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly

Explanation.-For the purposes of this section,-

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.[56]

According to Section 85 of The Information Technology Act,2000 states, that if any person contravenes any rule, the Act or any other direction every person who, at the time the contravention was committed, was responsible to, the company for the conduct of business of the company as well as the company, shall be considered guilty, and punished. A person shall be guilty of contravention, if the person proves that he had no knowledge of the contravention, or, he exercised his due diligence to prevent the contravention.

2. RBI GUIDELINES ON ONLINE BANKING

The Reserve Bank of India established a *Working Group on Internet Banking* to investigate various issues of Internet Banking. *The Group had focused on three major areas of banking, i.e, (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues"* . As a result, on June 14, 2001, the RBI published recommendations for banks to follow. All banks wanting to offer transactional services on the Internet were obliged to acquire prior clearance from the RBI under the initial internet banking rules. However, on July 20, 2005, this ban was lifted, and no previous permission from the Reserve Bank of India is necessary to provide Internet Banking services. . To guarantee compliance with RBI rules, institutions wanting to provide online banking should have a Board of Directors-approved online Banking policy.

Internet Banking Guidelines

"(i*) The bank should formulate a policy for Internet Banking with the approval of the Board.*

(ii) The policy should fit into the bank's overall Information technology and Information

[56] Ibid note 50.

 ISSN: 2582-6433

Security Policy and ensures confidentiality of records and security systems.

(iii) The policy should clearly lay down the procedure to be followed in respect of 'Know Your Customer' requirements.

(iv) The policy should cover technology and security standards and also address the legal, regulatory and supervisory issues as enumerated in this Annex.

(v) The banks should put in place sound internal control systems and take into account the operational risks involved in providing the service.

(vi) Adequate disclosure should be made regarding the risk, responsibilities and liabilities to the customers before offering the facility".[57]

3.THE CONSUMER PROTECTION ACT,2019

The preamble to the Act states-

"*An Act to provide for protection of the interests of consumers and for the said purpose, to establish authorities for timely and effective administration and settlement of consumers' disputes and for matters connected therewith or incidental thereto."*[58]

The purpose of this statute is to safeguard consumer interests. It is also be made applicable to banking services. This legislation protects the rights and obligations of consumers and banks regarding online banking, as well as problems related to privacy and the confidentiality of consumer accounts.

Whether there is a need of improvement in the laws relating to online banking?

Yes, there is a continuous need of improvement in laws relating to online banking in India. These changes are necessary so that laws evolve according to the changing technology. These changes are necessary so as to protect the consumers and to ensure the data security. The areas of improvements can be in the field of-

1. Maintaining strict cybersecurity standards in Online banking.
2. To promote financial literacy and consumer awareness among the masses relating to online banking.
3. Laws should be made to promote financial inclusion of the masses, including the poor and marginalised population.

[57] Guidelines on Internet Banking facility to Customers of Cooperative banks, rbi.org, Oct 21 2023 https://www.rbi.org.in/hindi1/Upload/content/PDFs/C229260416_1.pdf

[58] The Consumer Protection Act, 2019, No 35, Act of Parliament 2019(India),

 ISSN: 2582-6433

4. Clear laws should be made so as to promote Data privacy and security of consumers confidential banking information.

CHAPTER- 06

CASES IN REFERENCE TO ONLINE BANKING IN INDIA

1. The PNB Scam

On 14 Feburary,2019, Punjab National Bank reported India's largest bank fraud. The prime accuse in this case were, the diamond merchant Nirav Modi , his relatives and the PNB employees, who scammed PNB of Rs.11,400 crores. In this case, the bankers had issued fake Letter of Undertaking (LoU) at PNB's Brady House branch in Fort, Mumbai, making the bank accountable for any short-term loans taken out by the accused. PNB ignored the requirements, of giving out these LOUs exclusively in the event that the customer possesses collateral held by the issuing bank. Here, however, PNB issued the LOUs based on Modi's assurance. The PNB's Core Banking System (CBS), which is

 ISSN: 2582-6433

utilised for record keeping, did not record any of these transactions made by PNB and Nirav Modi. A corresponding entry was made, but a smaller value was quoted. In PNB's CBS framework. These illicit LoU-related transactions were all carried out via the SWIFT system by dishonest PNB personnel.

On March 13, 2018, RBI issued a notice prohibiting the banks from issuing guarantees in the form of Letters of Undertaking (LOU) to prevent any further misuse of this facility with immediate effect.

The RBI also ordered the SWIFT system to be linked with the banks' record-keeping system, the Core Banking System (CBS), by the deadline. The Nirav Modi case, is generally related to Indian Banking system , and not specifically related to Online banking in India.

2. Akhilesh Kumar Singh v/s Bharti Airtel Limited & Another(2013)

The facts of the case are that, the appellant was having a mobile connection from Bharti Air Tel Ltd. He also had one account in the 'State Bank of India 'and the mobile number of the appellant was registered with the account number of the appellant. It was alleged that on 21.08.2011 a total amount of Rs.1,40,000/- was transferred from his account fraudulently and he got three SMSs alert on his mobile indicating that Rs.45,000/-, Rs.55,000/- and Rs.40,000/- were transferred from his account through internet banking. As the above fund transfers were not authorised by him neither had he carried out any transaction through internet, amount should not have been debited from his account. It has been alleged by the complainant that this could happen as the Bharti Airtel Ltd. disconnected mobile phone of the complainant and gave the sim to some other customer who fraudulently withdrew this amount. The complainant filed the criminal complaint against the opposite parties and also filed an application before the Banking Ombudsman for recovery of the debited amounts. Here, the Banking Ombudsman ordered for the payment of the compensation.

The complainant, herein the opposite party contested the application. The State commission herein decided that the complaint wasn't maintainable and hence was dismissed.

CONCLUSION

Banking, the lifeline of India's economy has seen a revolutionary and a tremendous change, with the introduction of online banking. Online banking, also called as electronic banking, internet banking, etc., is performing the conventional banking services over the internet

 ISSN: 2582-6433

platform. It has benefited both the Customers and the bankers. The trends of online banking have continuously evolved. New trends of banking include, Mobile banking, NEFT,RTGS IMPS, UPI etc. With the changing trends in the online banking structure, new laws have come up to govern the online banking in India, like The Information Technology Act, 2000 , Consumer Protection Act,2019.

BIBLIOGRAPHY

1. Uppal R.K and Jha N.K(2008), Online Banking in India, Anmol Publications Pvt Ltd.
2. Nagarajan Vivek and Selvan Ambu Samuel; Indian Scenario of E- banking
3. Journal Legal framework on the Internet Banking in India by Rohit Jain, International Journal of Law Management and Humanities (ISSN 2581-5369): Volume 4 Issue 1 ,2021
4. Journal, 'Anytime, Anywhere, Anyway': Online Banking offers greater convenience and easier financial planning by Jon Newberry published in ABA Journal, Vol 82, No.12 (December 1996)