INTERNATIONAL JOURNAL OF LEGAL ENFORCEMENT

ISSN: 2582 8894|UIA: AA1003/2020

Volume 1 Issue 2

|June 2021|

Website: www.internationaljournaloflegalenforcement-ijle.com

Email: editorialboard.ijle@gmail.com

INTERNATIONAL JOURNAL OF LEGAL ENFORCEMENT
ISSN: 2582 8894|UIA: AA1003/2020

About Us

International Journal of Legal Enforcement is an online peer review journal dedicated to express views on legal and socio legal aspects. This platform also shall ignite the initiative of the young students. We do not charge any publication charge for online publications. We process to bring out the analysis and thoughts of every socio legal and legal matters from the young powerful minds. With this thought we hereby present you, International Journal of Legal Enforcement.

"Dharma is to protect the Needy"

INTERNATIONAL JOURNAL OF LEGAL ENFORCEMENT
ISSN: 2582 8894|UIA: AA1003/2020

Research Article on

INTERNET BANKING FRAUDS AND INDIAN LEGAL PERSPECTIVE

Pallavi Nayyar

Student, Amity Law School, Noida

ABSTRACT

The World Banking sector due to globalization, liberalization and privatization has influenced and created a competitive environment. Every sphere of a human being's life is influenced by information technology. This technology has played a major role in improving banking services and has brought about distinctive changes in Indian Banks. This technology gives remedies for solving today's problems related to the banking sector. The increasing rate of transactions has created challenges and problems in the banking sectors. Electronic medium for banking helps to provide easier transactions and also saves the time of the people. Internet banking means the complete sphere of technology initiatives that have taken place in banking industries which can be availed by people sitting at home.

This research paper's scope is to analyze the scope and limitation of internet banking and their frauds relating to issues in Indian Banking. This research paper will cover aspects of banking frauds in light of cyber law and information technology law and study the concept of internet banking from an Indian Legal perspective.

MOTIVE OF ARTICLE: To study and understand the laws and problems related to internet banking as per Indian Legal Perspective, frauds and their prevention. This paper's objectives are:

- To understand different types of frauds being committed in internet banks.
- To analyze the legislative framework which prevents banking frauds in India.
- To know the important role played by the Reserve Bank of India in Internet Banking.
- To highlight different security issues relating to internet banking in India.

Acts and various enactments governing trade and commerce, dealt in this paper :

- Indian Penal Code, 1860
- Indian Contract Act, 1872
- Negotiable Instruments Act, 1881
- Reserve Bank of India Act, 1934
- Banking Regulation Act, 1949
- Information Technology Act, 2000

INTRODUCTION

"DIGITAL PAYMENT SYSTEMS CAN DO MORE FOR EQUALITY IN POOR COUNTRIES THAN THEY CAN DO ANYWHERE ELSE, AND WE WOULD LIKE THEM TO EMERGE THERE EVEN IF IT TAKES LONGER IN RICHER COUNTRIES. WE ARE NOT WAITING FOR IT TO TRICKLE DOWN AS WE DO FOR MANY ADVANCED TECHNOLOGIES"

-BILL GATES

The concept of internet banking in India is a very recent concept. Now the old and traditional manual system of banking facilities is not practised. The complete credit for bringing about the change in the Banking system of India to the internet system goes to private Banks like CitiBank, HDFC Bank, ICICI Banks, etc. These banks follow the Internet Banking System and now the internet banking system is established in India also. Internet banking was introduced by Citi Bank or HDFC Bank in 1999.[1]

Banking over the internet has attracted the attention of bankers and other financial services, industry participants, lawmakers, etc. among the reasons for internet banking's audience are the notion that internet banking payments will grow rapidly, industry projections that internet banking will cut bank's cost's increases Bank revenue growth and also will make banking convenient for customers.

a) HISTORY OF INTERNET BANKING

With World Wide Web Development the concept of internet banking started. Some Internet Technology people working on Banking databases came up with the new idea of online Banking Transaction in the 1980s that is online shopping, even a credit card helps to promote the concept of online Banking. In India Internet Banking is a novel concept. In India, the traditional banking system was running through the branch banking system. In 1990, the concept of the non-branch banking system started. This novel concept of internet banking became more popular with time over the old traditional manual branch banking system.

Banks of internet banking are of two types:

[1] ibid

- A bank whose office is existing physically can establish a website and it can also offer to its customers the facility of internet banking in addition to its traditional services.
- It can establish a 'virtual', 'branchless' or 'internet-only bank. The computer server which lies at the heart of the virtual bank may be housed in an office that serves as a legal address of such a bank or some other location.

The Government of India also enacted the Information Technology Act, 2000. This act recognizes electronic transactions and other means of electronic commerce. This whole thing is being monitored and reviewed by the Reserve Bank of India. This bank reviews and monitors the legal and other requirements of internet banking continuously to ensure that internet banking would develop on sound lines and also Internet Banking related challenges do not pose a threat to financial stability. New schemes and technologies are introduced by private banks for the people and it makes a strict competition for public banks.

b) MEANING OF INTERNET BANKING

It is a method of banking in which all the transactions are conducted electronically via the internet. In this, payments can also be made through internet banking.

c) SCOPE AND LIMITATION

The scope is to analyse internet banking and their frauds relating to issues in Banks of India. Here the Indian Legal Perspective of Internet Banking will also be discussed. Here, we are going to analyse types of banking frauds, legislative framework and vigilance system adopted by Indian Banks and also some cases related to these.

When we actually see the perspective of banking products and services, it is being offered through the internet, internet banking is little more than traditional banking services which are delivered through an electronic communication backbone that is the internet.

ADVANTAGES:

- Through Internet Banking we can check our transactions at any time of the day and as many times as possible whereas in traditional methods we get quarterly statements from the bank.

- If fund transfer has to be made at an outstation where the bank does not have a branch, the branch would demand out stationed charges whereas in case of internet banking it is absolutely free.
- It is cost-effective and thousands of customers can be dealt with at the same time.
- There is no need for many clerks and cashiers and administrative work also gets reduced with internet banking.
- Expenditures on paper slips, forms, bank stationery, etc. have reduced, which helps to raise the profit margin of the banks.
- As customers are concerned, their account information is available 24x7 regardless of their location.
- They can reschedule their future payments from their bank accounts sitting far away.

d) LEVELS OF INTERNET BANKING SERVICES

Broadly speaking, the levels of banking services provided through the internet can be categorized into three types :

- THE BASIC LEVEL SERVICE is the bank's websites that disseminate information on different products and services offered to customers and members of the public in general. Through email, it can receive and reply to the queries of customers.
- THE SIMPLE TRANSACTIONAL WEBSITES allow different services queries of customers regarding the submission of their instructions, applications on their account balances, etc, and it does not do any transactions on their accounts which are a fraud.
- This banking service is offered by FULLY TRANSACTIONAL WEBSITES which allows the customers to operate on their accounts for the transfer of funds, payments of different bills, subscribing to other products of the bank and also to transact purchase and sale of the security.

All the above forms of Internet Banking services are offered by traditional banks as an additional method of serving the customer or even by the new banks who deliver banking services only through the internet or other electronic delivery channels as value-

added service. Some banks are known as 'virtual' banks or 'internet-only banks and they do not have any physical presence in our country though they are offering different banking services.

- The Narasimham Committee was instrumental in enforcing Indian Banks to become more competitive. The private sector banks forced the public sector banks to embrace technology so as to improve their level of customer service.
- The Khan Committee recommended the setting up of universal bank preference was given to financial institutions which provide a whole range of corporate finance solutions under one go.
- The Verma Committee – This committee recommended that even in weak public sector banks there is the need for greater use of information technology

e) RISK ARISING IN INTERNET BANKING

The Internet as an electronic medium is one of the biggest attractions due to its openness and freedom in the public domain and there is no restriction as to who can use it as long as one adheres to technical parameters.

Although there is a reduction in the cost of transactions, it has brought new orientation to risks and even new forms of risks to which banks conducting internet banking expose themselves. This technology plays a significant part both as a source and tool for the control of risks.

Operational risks/transactional risks are one of the most common forms of risk which are associated with internet banking. It deals with inaccurate processing of transactions, data privacy and confidentiality, compromises in data integrity, non-enforceability of contracts, unauthorized access/intrusion to bank's systems and transactions etc. These risks are due to improper designing, implementation and monitoring of information systems of banks. Apart from shortcomings in technology, human factors like negligence by employees and customers, the fraudulent activity of hackers, employees etc. can become an important source of operational risk.

Security risk arises when there is unauthorized access to critical information of a bank's stores like risk management system, accounting system, portfolio management

system, etc. A breach of security could result in a direct financial loss to the bank. For example, hackers operating through the Internet can implant a virus, retrieve, also use confidential information of the customer and also can access.

Other risks are infringing on the privacy of customers', loss of reputation and its legal implications. Controlling access to banks' systems is very important and it is very complex in the Internet environment which is in the domain of the public. Attempts at unauthorized access can emanate from any source and from anywhere in the world with or without criminal intent.

CHAPTERIZATION

CHAPTER 1: FRAUD IN THE INTERNET BANKING SECTOR

Fraud is defined as any behaviour by which individual goals for the achievement of unscrupulous preference over another and illegitimate loss to the other and illegitimate

causality to the other. Section 421[2] of the Indian Penal Code and Section 17[3] The Indian Contract Act defines Fraud. Fraud considered forgery-counterfeiting, cheating, breach of trust and concealment.

Internet fraud refers to 'online fraud'. It is a type of fraud scheme that uses email, chat rooms, websites or message boards to present fraudulent solicitations to prospective victims, to transmit the proceeds of fraud to financial institutions or to others connected with the scheme or to conduct fraudulent transactions. Internet banking fraud is a theft committed using online technology to illegally transfer or remove money from it to another bank account.

Types of internet banking fraud that can happen through smartphone, tablet and other mobile devices are:

- Phishing – It involves using a type of spam to fraudulently gain access to internet banking details of people. The word 'phishing' is basically the use of spam emails falsely claimed to be from a bank, in this manner criminals 'fish' for legal login information of bank customers.

  Millions of these emails fraudulently are sent by criminals at random email addresses with the hope of trapping unsuspecting innocent people into providing their personal banking details of banking. Generally, a phishing email asks an internet banking customer to follow a link to a banking website that is fake and asks him to also enter his or her personal details of the bank. If the customer follows the link, he becomes a victim because he also downloads a false program that captures his/her keyboard strokes which includes any typed information such as login details of bank and sends them to a third party.

  Phishing emails not only targets internet banking customers but also targets online auction sites or other online payment facilities. Such e-mails are not sent by legitimate banks to their customers.

[2] Dishonest or fraudulent removal or concealment or concealment of property to prevent distribution among creditors

[3] Fraud defined

- Mule recruitment – It is an attempt to get a person to obtain funds that are stolen using his or her bank account, and then transfer these funds to criminals. Generally, criminals have the tendency to send millions of jobs that are fraudulent and they send employment emails to random email addresses, in the hope of trapping unsuspecting innocent people in their criminal activity. If you have received the money in your bank account, transferred or attempted to transfer money overseas under these circumstances, please contact your financial institution immediately. Depending on the situation, it is possible that people who accept to participate in this kind of 'jobs' may be prosecuted.

CHAPTER 2: LEGISLATIVE FRAMEWORK

a) Indian Penal Code, 1860

The term 'fraud' does not categorize banking fraud as a distinct offence. Indian Penal Code defines forgery under Section 463[4], one can be said to commit forgery if he/she with the intention to cause damage or injury makes any false document. In order to constitute forgery, the intention of the one who is committing such an act must make the document with an intention that is fraudulent or dishonest.

b) Indian Contract Act, 1872

Section 10 of the Indian Contract Act states a contractual relationship exists between the customer and a banker. Hence, it can be said that the Act will be applicable to some extent in dealing with banking frauds in India.

Section 16 of the Act states that under the influence can be in a way categorized as a lesser degree of fraud.

Section 17 of the Act deals elaborately with the concept of fraud.

Section 18 deals with misrepresentation. In Oriental Bank Corporation v. John Flentming[5], the court analysed the concept of constructive fraud.

Section 19 states the voidability of agreements without free consent.

c) Negotiable Instruments Act, 1881

Section 131[6] The Negotiable Instruments Act says that the group holds the view that there is an obligation on the banks not only to establish the identity but also to make enquiries about the integrity and reputation of the prospective customer. The Group, therefore, endorses the present practice but has suggested that after coming into force of the Information Technology Act, 2000 and digital certification machinery being in place, it may be possible for the banks to rely on the digital signature of the introducer.

d) Banking Regulation Act, 1949

This does not deal with banking frauds directly in the banking sector. However, the provision under this Act somewhat helps one in understanding the operations of the banking business which in turn might help in understanding the reasons behind the occurrence of banking frauds. Central Government may be recommended by the Reserve

[4] Forgery
[5] (1879) 3 Bom. 242,287
[6] Non-liability of banker receiving payment of cheque

Bank of India for notifying the business of certifying authority as an approved activity under Section 6(1)(o)[7] of the Banking Regulations Act, 1949.

e) Information Technology Act, 2000

The Information Technology Act 2000, along with amending the Indian Penal Code to bring within its scope conventional offences committed electronically, has also created a new breed of technology offences, the prevention of which is incidental to the maintenance of a secure electronic environment for internet banking and for prevention of banking frauds and forgeries. A security procedure is required to be recognized by law from a legal perspective, as a substitute for signature.

The Information Technology Act, 2000 in India:

- Section 3(2): Provides for a particular technology as a method of authenticating records electronically. This has raised the doubt whether the existing methods are recognized by law used by banks as a valid method of authentication.

  Section 3(2) of the Information Technology Act, 2000 needs to be amended to provide that in addition to the procedure prescribed therein or that may be prescribed by the Central government, a security procedure of an electronic document/transaction during the transition period should be recognized as a valid method of authentication if it is mutually agreed to by the concerned parties.
- Section 21: Banks may be allowed to apply for a license to issue the digital signature certificate and function as certifying authority for facilitating Internet banking.
- Section 43: It has provided a penalty for denial of access to the computer system.
- Section 66: It has provided a penalty for denial of access to the computer system.
- Section 72: It has provided for the penalty for breach of privacy and confidentiality.
- Section 79: It has also provided for exclusion of liability of a network service provider for data travelling through their network subject to certain conditions.

CHAPTER 3: ROLE OF RESERVE BANK IN INTERNET BANKING

[7] Any other form of business which the Central Government may, by notification in the Official Gazette, specify as a form of business in which is lawful for a banking company to engage.

Many initiatives have been taken by the Reserve Bank of India and they have put forth guidelines for internet banking. They periodically review them. RBI approval must be taken by all banks before offering any internet transactional services. 'Working Group on Internet Banking,' recommendations were adopted by the RBI. They examined three thrust areas that are Legal issues, Regulatory and supervisory issues, Technology and security issues. Certificates from specialised external auditors are required by all banks which certifies their security control and procedures and has to submit this certificate periodically to RBI. Every breach or failure of security systems and its procedure, later on, its discretion may be reported to the banks.

The supervisory concerns on Internet banking are to a great extent the same as those of electronic banking. The guidelines of RBI which are given on 'Risks and Controls in Computers and Telecommunications' will be equally applicable to Internet banking. The complete risks associated with internet banking as a part of its regular inspections of banks are covered under the supervision of the RBI and it develops the required expertise for such inspections. This function is outsourced by RBI from qualified EDP auditors till this facility is built up in RBI.

The major supervisory focus of RBI is to maintain the record and also to provide availability for inspection and audit. The RBI's guidelines will need to be updated on 'Preservation and Record Maintenance' to include risks increased by banking on the net. The enhancements will include access by only authorized officials to an electronic record and regular filing of data, a sufficiently senior officer to be in charge of field data with well-defined responsibilities, proper software platform and tools should be used to prevent unauthorized alteration of field data, the data should be available on-line, etc.

Outsourcing guidelines should be developed by banks to manage systematically and effectively, third party service risks arise and it provides risks of disruption in service, defective services and service providers personnel gain intimate knowledge systems of the bank and can misutilized the same, etc.

A panel of auditors is provided by the RBI who will be required to certify the entire infrastructure security of both that is at the payment gateway end and also in the participating institutions before making the facility available for use by customers.

CHAPTER 4: ROLE OF CYBER CRIME COUNSEL IN BANKS

Digital wrongdoing can be explained as a violation that includes a place of wrongdoing, instrument, source, PC, target and a network as a medium[8]. With the increased digital transactions in business, wrongdoings floated towards a more advanced world. All around these types of digital assaults are increasing and in India, there is a sharp increase in digital violation cases in the previous few years. Juniper Exploration's investigation evaluated, in 2016 that expenses of cybercrime throughout the world could be as high as 2.1 trillion by 2019[9]. The online wrongdoings can be classified as:

- Hacking: It is unlawful to access a system to degenerate or to see any misguided information.
- Phishing: It includes a procedure to collect private data like username, password, one-time password etc.
- Vishing: A criminal act for social designing via phone to access individual and budgetary data from the population with the goal to attain monetary benefits.
- Spamming: Spontaneous messages sent to a mass population trying to constrain the message in individuals who might not get it.
- ATM Skimming and Purpose Offer Wrongdoings: It is the most developed method of the trading ATM machine. Effective execution of skimmers through ATM gather the card numbers and personal information that are later repeated to do fake transactions

At whatever point digital extortion is carried out the unfortunate casualty should answer to the Digital Misrepresentation Gathering that must be set up by every single bank to audit, screen research and report about digital wrongdoing. In the event that such Committee does not perform or declines to play out its obligation then an arrangement to record an FIR must be made. The Committee will act very fast in the case when the esteem is very high. RBI in its 2011 report expressed that when bank fakes are short of one Crore then it may not be important to require the consideration of the Extraordinary Advisory Group Board.

CHAPTER 5: INTERNET BANKING SCAMS

[8] Kharouni, L (2012) Automating Online Fraud Automatic Transfer System : The Latest Cyber Crime Tool Kit

[9] Liu, J., Hebenton B and Joy, S Handbook of Asian Criminology

The different types of internet banking scams that we observe are:

- Payment card fraud - There are many kinds of card fraud that are aimed at stealing your debit or credit card details, which involve either the stealing of the card itself or of the very important information present in the card. This will happen if you are not present during the time of the transaction, for example, when through the internet purchase is made, or if the card is not in your sight. Alternatively, you think that you are talking to a trusted organisation not realizing that it is a scammer to whom you are talking and he may trick you to provide the information, or even copy illegally the information from the magnetic strip present on the card and create a card which is 'cloned' with your details on it.
- Phishing' scams - This happens when scammers try to obtain your private, very important information, such as usernames, PIN, passwords, sometimes even money, and credit card details by pretending that he is from your bank or from the financial institution, a company who regularly does business with you, or from social networking site of yours. They can do this via the web page, email, phone call or text message. The details to access your account must be given only when scammers will give you some reason why they need this information. Generally, the reason used is that there is some problem with your account, and also to increase the chances of a response, the message may indicate a sense of urgency or there is the immediate risk if we fail to answer, to our bank account or to our credit card. Phishing emails generally include logos which are a copy of some official-logos, and it might also include convincing details regarding your personal history, which the scammers were able to obtain from the pages of your social networking. This might also include links to 'cloned' or 'spoofed' websites, which appears to be the genuine website of the financial institution, and which if you follow, you will be asked to enter personal information. Remember, if you receive any anonymous emails (or text messages), if it looks suspicious, delete it.

CHAPTER 6: CASES

a) Mr. Akhilesh Kumar Singh V. Bharti Airtel Ltd.

CASE DETAILS:

- Appellant: Mr Akhilesh Kumar Singh

  Respondent: Bharti Airtel Ltd.
- First Appeal No. 403 of 2014

  Decided On: June 21, 2019
- At National Consumer Disputes Redressal Commission NCDRC
- By, THE HONOURABLE MR. PREM NARAIN PRESIDING MEMBER

FACTS:

- The appellant was having a mobile connection from the respondent. He had an account in the State Bank of India and the mobile number of the complainant was registered with the account number of the complainant. On August 21, 2011, it was alleged that a total amount of Rs. 1,400,000/- was fraudulently transferred from his account for which he got three SMS on his mobile indicating three transactions from his account through internet Banking. This transaction was not authorized by him and he did not carry out any such transaction. So there should be no debt of such transaction amount from his account. The complainant alleged that this could be possible as the opposite party disconnected the mobile phone of the customer and gave the SIM to another customer who fraudulently withdraw this amount. A criminal complaint was filed by the complainant against the opposite parties and an application was filed before the Banking Ombudsman for recovery of the debited amount.
- The bank could recover only Rs.85,000/- which was given to the complainant. The Banking Ombudsman widened its order dated January 10, 2012, for the payment of Rs. 55,000 as the balanced amount.
- The aggrieved appellant filed a consumer complaint under the Consumer Protection Act before the State Commission. The complaint was contested by the opposite parties. The opposite parties filed an application stating that the case was not maintainable under section 7B[10] of the Indian Telegraph Act, 1885. The application was contested by the complainant and the State Commission

[10] Arbitration of disputes

ultimately decided that the complaint was not maintainable and hence it was dismissed.

JUDGEMENT: The Apex Court had observed Delay Condoned based on the decision rendered by the National Consumer Disputes Redressal Commission in the revision petition of 2013 decided in May 2014, was of the view that the petition filed by the petitioner is maintainable. The parties again appeared before the National Commission on October 10, 2017. Since opposite parties are not a Telegraph Authority, Section 7B is not applicable in the case and hence the order of the State Commission is not legally sustainable and hence liable to be set aside. Hence, the petition of complaint stood dismissed on June 21, 2019.

b) Seema Devendra Puranik V. Bank of Maharashtra

CASE DETAILS:

- Appellant : SEEMA DEVENDRA PURANIK
  Respondent: MR. AJAY BANERJEE [as he is the PIO and Chief General; Manager (Planning development and Corporate services) of Bank of Maharashtra]
- APPEAL NUMBER: CIC/SG/A/2011/002066
- DECISION NUMBER: CIC/SG/A/2011/002066/15525

FACTS:

By Phishing fraud the bank account of the appellant had been defrauded of Rs. 17,000. The appellant had asked for the information about an account to which her money had been diverted. The PIO claimed an exemption under Section 8(1)(j) of the Right to Information Act. The Commission agrees that information relating to the customer of a bank is exempt from disclosure when a fraud has occurred there is a larger public interest in the disclosure of the Information. So as per the provision of Sec 8(2) of the Right to Information Act, the Commission directs PIO to provide information regarding queries.

JUDGEMENT: The appeal was allowed. The decision was allowed in the open chamber. The PIO was directed to provide information as directed above to the appellant before November 30, 2011.

c) Mrs Sucheta Charudatta Dhekane V. Bank of Maharashtra

CASE DETAILS:

- Appellant : MRS. SUCHETA CHARUDATTA DHEKANE

  Respondent: MR. AJAY BANERJEE [as he is the PIO and Chief General; Manager (Planning development and Corporate services) of Bank of Maharashtra]
- APPEAL NUMBER: CIC/SG/A/2011/002073
- DECISION NUMBER: CIC/SG/A/2011/002073/15529

FACTS:

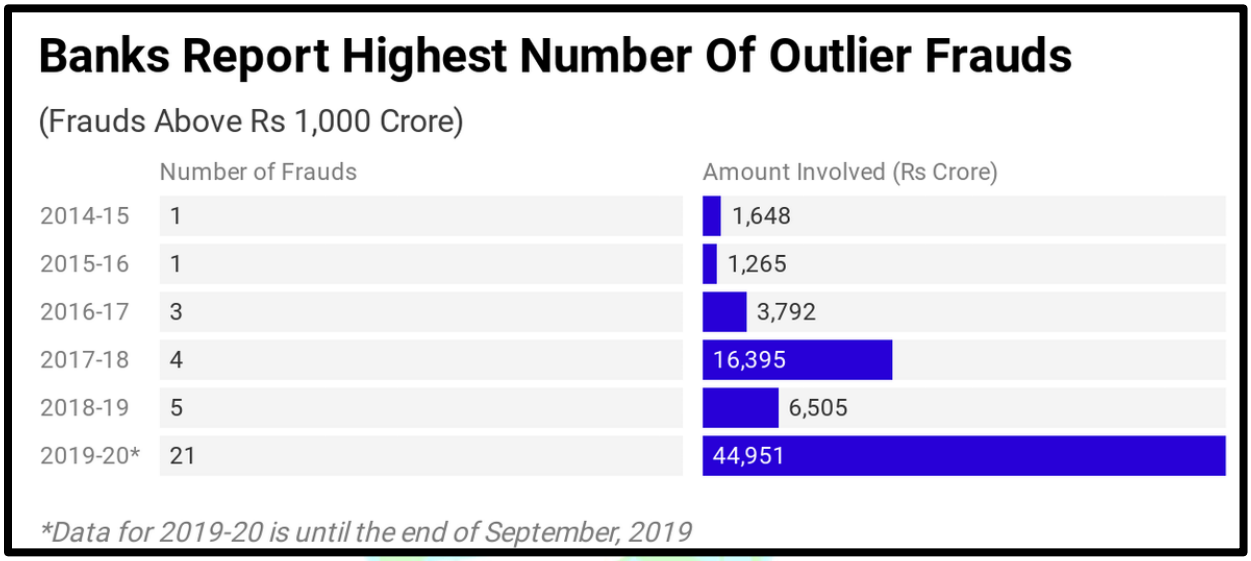
In this case, the money mule instances happened during June/July 2010, the accounts from the date of opening to information regarding the victims and their account details freezing of the account can not be provided as the information would impede the process of investigation or apprehension or prosecution of the offenders and as such exempt under Section 8(1)(h) of the Right to Information Act. However, regarding phishing, the account bank had made correspondence. The CPIO did not give complete and true information. The PIO had provided certain information regarding the queries.

JUDGEMENT: The appeal was allowed and the PIO was directed to provide information as directed above to the appellant before November 30, 2011.

CHAPTER 7: IMPACT OF COVID -19 ON INTERNET BANKING

According to the recommendations given by doctors and WHO, the most effective way to overcome the COVID-19 epidemic is to avoid ant personal contact which means that the movement of people has to be reduced and possibly advised to stay at home. In such a situation, most of the Banks in affected countries reduce their opening hours and

they also recommended to their customers to use internet banking as it is safe. To encourage the use of internet banking many banks have taken the opportunity to send messages which are positive and also to remind the users of the benefits of online banking. In this, the transactions can be carried out easily round the clock and they can enjoy permanent access to financial information. The customers also prefer to go in for internet banking so that they fear that cash could be unsafe and could spread coronavirus. This situation has become a turning point in the market.



With an increase in internet banking there is also an increase in internet banking frauds as a number of people have lost their jobs and they have no means by which they can survive along with their family members. As per the above graph, we can see that the number of frauds in the Year 2019-2020 has increased tremendously.

CONCLUSION

In the Internet Banking System, information is considered to be an asset and also worthy of protection. But, the present system of authentication does not address the security aspect completely. It calls for an urgent need to adapt to the whole system. According to the online banking association, member institutions rated security as the most important

issue of online banking. There is an important requirement to not only protect the privacy of the customers but also to protect them against fraud. Another issue that is arising is Data Protection and the need for a legal and regulatory framework.

Internet Technologies not only brings about change and transformation in Banking but it also brings a change and transforms into all aspects of finance and commerce. No crime should be tolerated. The safety and privacy of an individual should be safeguarded and every person has the right to live in an environment that is secure, whether it may be real life or the internet.