Page 794 - 808 **DOI:** *https://doij.org/10.10000/IJLMH.116243*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

Cyber Frauds: A Growing Threat to Indian Banking Sector & Preventive Strategies

DR. DINESH DAYMA[1]

ABSTRACT

The most dramatic revolution in payment methods in the past few decades has, undoubtedly, ben the plastic card and online banking services. The online banking services and card payment vehicle of convenience, which provides its users with multifarious benefits. The online banking fraud become one of the major challenges for today's banking system in India. Its involves the illegal banking activities such as fraudulent transfer fund, data theft, hacking and phishing etc. Online Banking Fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Indian cyber space has witnessed significant rise in cyber-attacks/ fraud, massive probing and targeted attacks on IT assets are being witnessed. The Indian cyberspace is also being used to host Command and Control Servers in the data centres. Attempts have been noticed to attacks telecom infrastructure particularly, the routers and DNS. There have been cyber-attacks on the Government, public sector, banks, private sector IT infrastructure like website defacements, intrusions, network probing, and targeted attacks to steal some information, identity theft (phishing) and disruption of services. With the coming of new Information and Communication Technology and Internet and their growing misuse side by side, scenario has been totally changed. One hand new technologies have facilitated the commission of old crimes by the bed element and at the same time crimes have originated commonly called as cybercrimes. It is important to note that cybercrime is very easy to commit with little resources but damage caused could be very huge. Because of internet bad elements are getting better network and hence facilitating cybercrime. The use of a computer to carry out any conventional criminal act, such as fraud, is called cybercrime and is a growing means. Cybercrime is growing so rapidly, in fact that the federal government has created a handful of agencies to deal with computer related crimes. The paper is focused to study and highlights the types and behaviours of Online banking frauds that take place in our banking systems.

Keywords: *Cyber Crime, Internet Banking, Online Banking Fraud.*

[1] Author is an Assistant Professor of Law (Senior Scale) at Campus Law Centre, Faculty of Law, University of Delhi, India.

 [ISSN 2581-5369]

I. INTRODUCTION

In today's world the human activities tend to depend on more and more on technology, especially internet, computer and information technology. In twenty first Century, Knowledge Society, the way people interact and communicate with each other all over the globe has changed drastically due to globalization and e-revolution. In the techno-world, the Internet has been created as a social practice where an individual can interact, share information and providing knowledge, exchange information, doing business, and be involved in social and political debates through using the internet as a tool. The Internet has become new methods to describe anything connected with technology and techno-culture in our society.

Over the last years, the use of the internet drastically increased. When the first time the internet developed, the founding father hardly had any idea that the Internet can change itself into a pervading revolution. With the extreme use of the Internet, many things are worrying in the cyber world. Due to the unidentified nature of the Internet, it gives a scope of illegal activity especially criminal in nature with impunity and people with intelligence have been grossly misusing the internet to propagate criminal activities in cyberspace. In the present scenario, the Internet is the necessity of human beings and important because of its facilities almost all aspects of transactions (including banking transaction) and activities concerning the Internet, the World Wide Web and Cyberspace.

While some of the risks in the banking sector have always been there, they keep changing with the constantly evolving technology standards and regulatory framework. A majority of the banks in India offer online including mobile banking services. Most of the transactions are conducted via payment cards, debit and credit cards, and electronic channels such as ATMs. Consequently, both private and public banks as well as other financial institutions in India are becoming increasingly vulnerable to sophisticated cyber-attacks. The online banking fraud become one of the major challenges for today's banking system in India. Its involves the illegal banking activities such as fraudulent transfer fund, data theft, hacking and phishing etc., to gain the monetary benefit from the banking industry.[2] The Reserve Bank of India Annual Report 2018-19 indicates- 6,800 cases of bank fraud involving an unprecedented Rs 71,500 crore have been reported in 2018-19. A total of 5,916 such cases were reported by banks in 2017-18 involving Rs 41,167.03 crore. As many as 6,801 cases of fraud were reported by scheduled commercial banks and select financial institutions involving an amount of Rs 71,542.93 crore

[2] D.K. MURTHY, VENUGOPAL, INDIAN BANKING SYSTEM (IK International Publishing House Pvt. Ltd., 2006) 10-20.

 [ISSN 2581-5369]

in the last fiscal (increase of over 73 per cent in the fraud amount).[3] However, RBI report in 20219-20 indicates that Bank frauds increased by 15% in FY19; amount defrauded spikes 73.8%. The Report mentioned that public-sector banks (PSBs) accounted for the bulk of the frauds. The report also indicate despite government's efforts the amount involved in frauds has gone up by a whopping 73.8 per cent.[4]

II. ONLINE BANKING – A NEW CHANNEL OF BANKING TRANSACTION

The importance of Information Technology is one of the most valuable assets for any organization and any economic system. It is re-defining the ways of conducting business and communication and is shaping the interaction between producers and consumers for the sale and purchase of goods and services. The Internet and its global reach have created new opportunities. Its benefits can be measured in terms of enhanced processing speed, transmission rates, and access time.[5]

Unfortunately, however, despite the importance of IT to the economic system, the information revolution has brought both negative and positive changes to the business, international affairs, and daily life. The growth of the internet for example has greatly influenced the way and speed with which information is shared by both the "good" and the "bad". The revolution in IT and its attendant globalization of the market have introduced more and new forms of opportunity for criminals.[6] Economic or white-collar crime, as it is generally referred to, is a crime committed by a person of a certain social status in the course of his occupation. The economic crime occurs as a deviation from the violator's occupational role. Also, most of the laws involved or violated are not part of the traditional criminal code. Such crimes are corporate fraud, public fraud, tax evasion, goods smuggling, currencies forgery, credit card fraud, intellectual property infringement, and the more recent phenomenon of cybercrime.[7]

III. CYBER CRIME LEADING TO ONLINE BANK FRAUDS

Cyber-crime has been defined as an illegal act generally committed by deception or misrepresentation by someone who has special professional or technical skills for personal or

[3] Reserve Bank of India, HANDBOOK OF STATISTICS ON THE INDIAN ECONOMY (Department of Statistics and Information Management, Reserve Bank of India) (2017).
[4] Reserve Bank of India Annual Report 2019-20. Pg. 198-201
[5] Monica N. Agu, *Challenges of Using Information Technology To Combat Economic Crime,* 6 AFR. J. COMP & ICTs 31, 31-35 (2013).
[6] Nicola & Scartezzini, *When Economic Crime Becomes Organized: The Role of Information Technologies. A Case Study*, 11 CRIMINAL JUSTICE 343, 343-348 (2000).
[7] Deepa Mehta, *Economic Crime in A Globalizing Society: Its Impact On The Sound Development Of The State - An Indian Perspective*, UNITED NATIONS ASIA AND FAR EAST INSTITUTE FOR THE PREVENTION OF CRIME AND THE TREATMENT OF OFFENDERS (Jul.18, 2018, 9:45 PM) http://www.unafei.or.jp/english/pdf/RS_No66/No66_10VE_Mehta1.pdf

 [ISSN 2581-5369]

organizational financial gain or to gain an unfair advantage over another individual or entity.[8] Cyber-crimes comprise a broad range of illegal activities and they occur as a deviation from the violator's occupational role. Due to the rapid advances in technology, new impetus, and opportunities for these economic crimes have been provided. It has been observed that online banking frauds have continued to grow rapidly because of the technological advances especially the rise of E-banking and the expansion of the Internet. Examples of these crimes include credit card fraud, money laundering, intellectual property infringement, and the more recent phenomenon of cyber-crimes.[9]

The most prevalent form of online banking frauds is credit card frauds, which can be categorized in two forms- *behavioural fraud and application fraud*. Application fraud occurs when individuals obtain new credit cards using false personal information and spend as much within such period while behavioural fraud occurs when details of the legitimate card have been fraudulently obtained and sales made when the card holder is not present, for instance, in e-commerce which requires only the card details. The worst casualty of internet vandalism is perhaps the economy. The impact of the network technology on the economic world and so great is its speed that an oft-quoted estimate is that UK's currency reserves could be transferred abroad in 15 minutes.[10]

In the last few decades, electronic commerce has become a major buzzword in the information society. The UK Department of Trade and Industry defines the e-commerce concept as follows: "*using an electronic network to simplify and speed up all stage of the business process, from design and making to buying, selling and delivering*." Over the years there has been a significant change in the types of frauds affecting the banking industry. With the introduction of new technology and channels for customers, it is becoming increasingly critical for banks to function. However, a cursory glance at the responses received, indicate that traditional fraud typologies still play a significant role in the types of frauds committed as well as the subsequent fraud loss that occurs. There are following different types of cybercrime especially, related to online banking frauds-such as Hacking, Phishing, Internet frauds, malware, data diddling, information theft, identity theft, malware, etc.

1. Hacking into Computer

[8] V. Rajendran, *Banking on IT's Security,* JOURNAL OF INDIAN INSTITUTE OF BANKING AND FINANCE, January-March 2018, at 13,17.

[9] Council of Europe Committee of Ministers, Recommendation No. R (81) 12, Adopted by the Committee of Ministers on 25 June 1981at the 335th meeting of the Ministers' Deputies. "*Report of the European Committee on crime problems on Economic Crime*", (1981 p.16)

[10] FERRERA, LICHTENSTEIN, REDER, AUGUST AND SCHIANO, CYBER LAW: TEXTS AND CASES, 241 (2002).

 [ISSN 2581-5369]

The term '*computer hacking'* traditionally described the penetration of computer systems, which is not carried out with the aims of manipulation, sabotage, or espionage, but for the pleasure of overcoming the traditional technical security measures.[11] However, with the increasing use of computer networks by commercial organizations, the potential of hacking was realized by criminals and it became the basis for almost all types of cybercriminals.[12] The hacking technique depends upon the respective communication and security system that is used by a network or a computer.[13] Traditionally, a form of hacking was based on the use of the standard password, physically watching the user typing in the details or using confidence tricks by which the hacker persuades or deceives the user to revel them. Though awareness about better password management has come about in the computer users, the advent of the Internet has brought many new techniques that are used in hacking and computer manipulations. The major techniques that are used by the hacker to get entry into a computer system are as follows:

a) **IP- SPOOFING:** This technique is used to gain unauthorised access to computers or networks from outside by pretending to be an authorised and trusted device inside the penetrated network. This is done through the modification of IP addresses in data packet headers transmitted to an incoming port of the network's router. Although the fake IP address is known as a valid address inside the network only, routers are not able to distinguish between data transmitted from outside or inside the network. Newer routers and firewalls offer protection against this kind of attack.[14]

b) **DNS SPOOFING:** DNS spoofing described the faking of host-masks during the resolution of the internet hostname. DSN or "*Domain Name Service*" provides the mapping between the hostname and IP address. Every access request on the internet using the host-name had to be resolved to its IP address, which is done by communicating with a DNS-server which stores the host-masks in databases. To perform the DNS spoofing attack, a hacker tries to intercept the communication and to send fake hostname mappings to the victim's computers. Once the applet is activated, the user's communication can be rerouted and the transmitted data can be gathered.

c) **WEB SPOOFING:** While IP and DSN spoofing depend on sophisticated technical knowledge, web-spoofing attacks use a much simpler approach. These are based on optical illusion in general. Hyperlink on a webpage can contain characters that make an

[11] D. P. MITTAL, LAW OF INFORMATION TECHNOLOGY (CYBER LAW),49-55(2000).
[12] *Id*.
[13] P. TAYLOR, *Hacktivism: In Search of Lost Ethics*, J. HUM. TTS PRAC., Nov. 2015, at 625-646.
[14]S. V. JOGA RAO, LAW OF CYBER CRIME AND INFORMATION TECHNOLOGY LAW, 194 (2004).

 [ISSN 2581-5369]

address look real, but in fact, lead to the wrong website e.g. Replacing the letter "o" in the address (www.micr0soft.com). Most users would not suspect any malicious intention. In this example, the hacker would set up a web-page asking for the input of sensitive user information. e.g. Credit card information.[15]

As per the Information Technology Act, Section 2(1)(v) of the Act[16] defines "information" includes data, text, images, sound voice, codes, computer programmes, software, and databases, or microfilm or computer-generated microfiche. The Indian Information Technology Act, 2000 makes hacking on offence. The provision contained in the Act is as follow: The Act[17] defines "hacking" thus: -

> ***Section 66: (1)*** *Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. Subsection (2) provides that the punishment for hacking is imprisonment up to three years, or with a fine which may extend up to two lacks rupee, or with both.*

Now broken down to its elements of section 66 proscribes as hacking require:

1. Destruction, deletion, or alteration of any information residing in a computer resource, or;
2. Diminution in the value or utility of such information, or;
3. Any act which injuriously affects the information by any means;
4. Any of the preceding acts should be with the intent to cause or with the knowledge of the likelihood of wrongful loss or damage to the public or any person.

Two points need attention to the consideration of this definition of hacking. One is that it is limited in scope and secondly this does not include all the offences that may be committed against computers or through computers. Under this definition, hacking would have taken place only when the information is a computer is destroyed or later or its value or utility is diminished or when that information is injured in any way. This should have been done with the criminal intent to cause wrongful loss or damage to the public or any person or with the knowledge that such loss or damage is likely to occur. Mere stealing of the information after entering into a computer system would not amount to hacking under this definition though access to that

[15] *Id.*
[16] The Information Technology Act, 2000, No. 21, Act of Parliament, 2000 (India).
[17] The Information Technology Act, 2000, No. 21, Act of Parliament, 2000 (India).

 [ISSN 2581-5369]

information would cause substantial loss to the individual or organization using that system. Stealing information by merely reading it or copyright it would be no offence because there is no destruction, deletion or alteration of the information. Of course, by exposure to an outsider, the values of the information to the person who has a proprietary interest in the information is diminished thereby causing loss, but the prescription of the offence is to be made more directly by making mere unauthorized access to a computer an offence with a monetary threshold level covering the loss. Criminal law on computer abuse should prohibit acts that would be inconsistent with the confidentiality, integrity, and availability of information stores in a computer.

In the United State legislation, the Computer Fraud and Abuse Act, 1986[18] regulates several criminal activities on the Net apart from "unauthorized access" to obtain sensitive information such as defence-related information and financial and consumer-used by or for the US government is also barred. Section 1030 (a) (5) (A) of the Act also prohibits the transmission of a "*programme, information, code or command to a computer or computer system*" with intent to damage or cause damage to, or to withhold or deny the use of computer services or network, information data, or program. Such transmission is also prohibited if done with reckless disregard of a substantial and unjustifiable risk of the same effect. India being a member of the information society not only relishes the fruit of technological advancements but like it's any other counterpart, it also exposes itself to breach of security and has been a victim of it umpteen times and even important government and scientific installations were not spared.

However, Indian legislation, Section 66 of the IT Act, 2000, i.e., before the amendment of 2008, carried the misleading heading of "Hacking" but the offence covered under the said heading was of deleting, destroying, or altering data residing in a computer or computer resource. *In Yates v. United States*,[19] Hon'ble Justice Kagan succinctly noted that "*the wise rule that the title of a statute and the heading of a section cannot limit the plain meaning of the text*,"[20] and refused to let the title sway interpretation of a statute or to override the laws' clear terms. Settled law in India is that marginal heading and notes cannot control the interpretation of when the section of law itself is clear and unambiguous.[21] The variations from the opinion voiced by Justice Kagan of the US Supreme Court is when a section or statute is unambiguous, in which case, the Supreme Court of India has held in several judgments that, the headings and marginal notes

[18] Computer Fraud and Abuse Act (CFAA) Pub. L. No. 99-474, 100 Stat. 1213 (Oct. 16, 1986), codified as amended at 18 U.S.C. §1030.
[19] Yates v. United States, 575 US 1002 (2015).
[20] Trainmen v. Baltimore & Ohio R. Co., 331 U.S.519, 528-529 (1947).
[21] Chandroji Rao v. Commissioner of Income Tax, M.P.(SC) 1970 AIR 1582.

 [ISSN 2581-5369]

may be referred to or relied on for purposive interpretation of statutes, quoting Maxwell on Interpretation of Statutes,[22] as: "*The heading prefixed to section or sets of a section in some modern statutes are regarded as preambles to those sections. They cannot control the plain words of the statute but they may explain ambiguous words.*" The Supreme Court has held that such deviation does not militate against the general rule but is intended for true and correct interpretation and application of statutory laws.[23] Applying the provision of Section 66, a case was registered for 'Hacking' against the owner of a webserver for blocking the site of a business, which had failed to meet its dues. The basis for the initiation of this prosecution is that the act of blocking the sites amounted to deleting, destroying, or altering information on a computer resource, with intent to cause harm and loss to the website's owner. This case is one of the classic examples of misuse of a provision and highlights the need for constructive and harmonious interpretation set out under section 66 of the Act.

In the case of *Syed Asifuddin*[24] case was registered against some representatives of Tata Indicom for unlocking of CDMA phone distributed by Reliance Info along with their mobile service package at nil to negligible cost. The unlocking was required to make the phones compatible for the competitor's networks. Cases were initiated under Section 66 of the Act. Similarly unlocking mobile phones, which are locked by telecommunication companies, which bundle such phones with services, was also exempted from the DMCA. This situation is similar to that of the Reliance case in India. The Copyright Act, 1957, does extend some instances of fair use but altering or modifying information on a computer resource was and continues to be an offence under the IT Act. Amendments of 2008, however, included *dishonest and fraudulent* intent as a precondition to making the above acts an offence. After the amendments came into effect on October 27, 2009, Section 43(a) read with the new Section 66 makes the acts constituting "*hacking*" a criminal offence.[25] Similarly, In the case of *State of Maharastra v. Rajkumar Kunda Swami*,[26] the accused a clerk at *Abhyudaya Co-operative Bank Ltd*. made wrongful gains of about Rs. 2.27 crore by opening a fake account in his name and the names of family members and by manipulating the credit entries by tampering with the computer data, he siphoned out the above sum through the fake accounts, money withdrawn from fake accounts and thus defrauded the bank. After releasing on bail, in this case, registered against him under

[22] P. B. MAXWELL, MAXWELL ON INTERPRETATION OF STATUTES 205-06 (10ed. 1953)
[23] Tata Power Company Ltd. v. Reliance Energy Limited, (2009) 16 SCC 659.
[24] Syed Asifuddin v. The State of A.P. & Anr. 2005 CriLJ 4314.
[25] In addition to the above provision, Section 43(g) makes an accomplice who assists any person to facilitate access to a computer, computer system or computer network in contravention of the Act, and rules or regulations made thereunder, also criminally liable.
[26] State of Maharastra v. Rajkumar Kunda Swami, 2001 SCC 1171.

 [ISSN 2581-5369]

Section 409, 420, 463, 464, 471, 477A of the IPC and under Section 43 read with Section 66, 65, 73 of the IT Act, the accused absconded and hence the Bombay High Court cancelled his bail. Considering these case laws can say that hacking is one of the mode to collect customer's information (especially bank account details) for committing crime such as online banking fraud in India.

2. Phishing:

Phishing is a financial crime, where a cyber-criminal poses as a genuine service provider and sends as an email requesting for updating record such as credit cards details, and acquires passwords. In the cyber-world, phishing [27](also known as carding and spoofing) is a form of the illegal act whereby fraudulently sensitive information is acquired, such as password and credit card details by a person/ entity masquerading as a trustworthy person or business in an official electronic communication such as an email or instantaneous communications. It is advisable to adopt reliable technology-based anti-dumping tools and a mechanism to gain general awareness on identifying vis-a-vis anti-phishing is a step in the right direction and will help to strengthen safeguard and proper interest of the Internet and deter possible offenders from committing phishing or similar online frauds.

- In the case of *NASSCOM v. Ajay Sood*,[28] the Delhi High Court applied the laws of misrepresentation to an illegal act of phishing committed by defendants' employees, who were part of a placement agency, who sent a letter and emails to NASSCOM. In this case, The Delhi High Court took notice of developing trends in the commission of frauds including phishing attacks online.
- In *Santosh Mandal v. State of Jharkhand*.,[29]the accused were charged with offences under Section 419,420, 467 and 471 of IPC and Section 66(A)(C)(D) of the IT Act. The accused had collected details of several ATM cards and PINs through phone calls to the victims. In some instances of this nature, the culprits would mislead the victims into believing they were calling from the bank by giving the first 12-digit number on the cards, which common to all cards issued by a service provider (like MasterCard or Visa). Two mobile phones and two papers recovered from the accused had the above

[27] In one such instance in August 2003 a bulk e-mail was received by customers of Citibank asking them to visit its official website and agree to change policies. The URL link www.citibank.com took place the recipient not to the Citibank site but to some other site where the user was asked to certain personal details. The UK strengthened its legal arsenal against phishing with the Fraud Act, 2006, which introduces a general of fraud that can carry up to three-year prison sentence and prohibits the development or possession of phishing kits with intent to commit fraud.

[28] NASSCOM v. Ajay Sood, 119 (2005) DLT 596: 2005(30) PTC Del.

[29] Santosh Mandal v. State of Jharkhand, 2015 SCC online Jhar 4637.

 [ISSN 2581-5369]

information culled through phone phishing which is otherwise referred to as "vishing". The application for bail filed by the accused was rejected by the Jharkhand High Court.

- In *Binod Kumar Mandal v. The State of the Jharkhand*,[30] the Jharkhand High Court rejected bail for the accused indicated in a case registered under Section 419,420, 467,468,471 read with Section 66A,66B, and 66D of the Act. The accused made withdrawals from the ATMs on daily basis using card details obtaining through calls to victims. The mobile phone recovered also assisted in the investigation as the call details to the victims were traced through the same.
- In *Suganathan v. The Superintendent of Police*,[31] two accused were attempting to withdraw money using fake ATM cards from the Canara Bank ATM centre, situated inside the Domestic Airport, Chennai. During the investigation, the names of other persons involved in the scam surfaced. Despite the seriousness of the above allegations, the accused were granted bail.

In Indian IT Act 2000 of section 66C and 66D prescribe punishment for identity theft and cheating by personation respectively which provides a maximum term of 3 years of imprisonment and fine up to one lakh rupee. In most phishing cases these provisions will be attracted apart from Section 420 of Indian Penal Code, 1860 for cheating.[32]

3. **Data Diddiling**: One of the most common forms of computer crime is data diddling – illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have affected banks, inventory records, credit records, and virtually all other data processing know.
4. **Salami Attacks:** Salami attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. For instance, a bank employee inserts a program into the bank's servers that deduct a small amount of money from the account of every customer. No account holder will probably notice unauthorized debit, but the bank employee will make a sizeable amount of money every month.
5. **Email bombing:** Email bombing refers to sending a large number of emails to the victims resulting in the victim's email accounts (in case of an individual) or email servers (in case of a company or an email service provider) crashing. Email bombing is

[30] Binod Kumar Mandal v. The State of the Jharkhand, 2015 SCC ONLINE Jhar 5007.
[31] Suganathan v. The Superintendent of Police, 2015 SCC online Mad 8330.
[32] § 420 The Indian Penal Code 1860.

 [ISSN 2581-5369]

a type of denial of service attack. A denial of service attack is one in which a flood of information requests is sent to a server, bringing the system to its keens and making the server difficult to access.

6. **Data Theft:** According to the Information Technology act, 2000 as amended by the Information Technology (Amendment) Act, 2008, Crimes of data theft under Section 43(b)[33] is stated as if any person without the permission of the owner or any other person who is in charge of a computer, computer system, computer network- downloads, copies, or extract any data, computer database or information from such computer, computer system, or computer network including information or data held or stored in any removable storage medium. Data theft is quite simply the unauthorized copying or removal of confidential information from a business or the other large enterprise. The term describes when information is illegally copied or taken from a business or the other individual. Commonly, this type of information is user information such as password and social security number, card details and other personal information, or other conditional corporate information. Because this information is illegally obtained when the individual who stole this information is apprehended, he or she will likely be prosecuted to the fullest extent of the law.

IV. LAW RELATING ONLINE BANKING FRAUDS

The Information Technology Act, 2000 for securing online transaction in banking industry as well as others preventing cyber-crimes in India, therefore certain amendment was made in some convectional laws such as The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Reserve Bank of India Act, 1934, The Banker's Book Evidence Act, 1891, The Negotiable Instrument Act, 1881 or wider interpretation is given to other.

1. The Indian Penal code:

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The sections dealing with a false entry in a record or false document etc. (e.g. 192, 204, 463, 464, 468 to 470, 471, 474, 476, etc.) have since been amended as '*electronic record and electronic document*' and thereby bringing within the ambit of IPC. After the amendment, the investigating agencies file the cases/charge-sheet quoting the relevant sections from IPC under section 463, 464, 468, and 469 read with the IT Act, under Sections 43 and 66 like offences to ensure the evidence

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

 [ISSN 2581-5369]

and/or punishment can be covered and proved under either of these under both legislation.[34]

Important Sections of India Penal Code Attracted in Cyber Crimes in Addition to Provisions Under Information Technology Act, 2000.

Waging was against Government of India- Section 121	Extortion- Section 383	False Electronic Evidence –Section 193	Defamation- Section 500
Promoting enmity between different religious groups Section 153A, 295A	Criminal breach of trust/fraud- Section 406 of IPC	Forgery of electronic record- section 470	Criminal intimidation-Section 503, 507
Theft- Section 379	Cheating by personation-419	Sale of obscene books- Section 292	Outraging modesty of women- Section 509
Receiving stolen computer resources- Section 411	Destruction of electronic evidence- Section 204	Criminal Conspiracy- Section 120B	Falsification of Electronic accounts- Section 477A

2. The Information Technology Act, 2000

The Information Technology Act 2000 as amended in 2008 regulates electronic business transactions and combat cybercrimes in India. The provisions of Act provide legal recognition is given to all electronic records through electronic signatures authenticated by the controller of Certifying Authorities after verification of the origin, destination, date and time of transition, following an audit of these matters. The offence of hacking and phishing covered under Sections 66 of the Information Technology Act[35] this offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.[36]

3. Indian Evidence Act 1872

A rapid increase in the use of computer and the internet has given rise to new forms of crime

[34] Rohit K. Gupta, *An overview of cyber laws vs. cybercrimes: in Indian perspective*, LEXOLOGY (June. 20, 2021, 11:00 AM) https://www.lexology.com/library/detail.aspx?g=c0dd03b8-fab9-4daa-be5b-40b723537899
[35] § 66 The Information Technology Act, 2000.
[36] § 77B The Information Technology Act, 2000.

like publishing sexually explicit materials in electronic form, video voyeurism and breach of conditionality and leakage of data by an intermediary, online banking frauds like personation commonly known as Phishing, identity theft, and offensive messages through communication services. So provisions were required to be included in the Indian Penal Code and Indian Evidence Act, and the Criminal Procure Code to prevent such crimes. However, section 65 A and 65 B of the Evidence Act[37] a special provision as to evidence relating to electronic record and admissibility of electronic records has been introduced with effect from 17th October 2000. Therefore, there is no bar of examination of a witness by way of video conferencing being an essential part of electronic methods.

4. The Reserve Bank of India Act, 1943

The Reserve Bank of India Act, 1934 was amended to grant legal reorganization and to facilitate electronic find transfer between the financial institution.[38] Moreover, every bank has to take RBI approval while initiating online banking services to the customers.[39] RBI introduce Electronic Fund Transfer scheme, this scheme offering customers money transfer services from one account to account of any bank, or any other branch in the place where EFT services are offered.[40] RBI plays an important role in online banking system by making it compulsory for the banks to route their high value transactions through Real Time Gross Settlement (RTGS)[41] and also by introducing National Electronic Funds Transfer (NEFT) and National Electronic Clearing Services (NECS).[42]

5. The Banker's Book Evidence Act, 1881

The Banker's Books Evidence Act, 1891 was amended so as given legal sanctity for books of accounts maintained in the electronic form by the banks. After the enactment of the IT Act, the definition part of the Bankers' Books Evidence Act stood amended as: Banker's book which includes the accounts books or day book or any other day books relating to banking business whether it may be in written form or in any electronic form. The electronic formats include the

[37] § 65 A The Information Technology Act, 2000. (Special provisions as to evidence relating to electronic record: The contents of electronic records may be proved in accordance with the provisions of section 65B (w.e.f. 17-10-2000)).
65B. Admissibility of electronic records.
[38] *Legal Framework for Electronic Banking;* THE RESERVE BANK OF INDIA, Date: 17 July 1999; https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=28
[39] N P Singh, *Online Frauds in Bank with Phishing* 12: 2 J. INTERNET BANKING AND COMMERCE, (August 2007) (June. 15, 2021 10:30 AM) www.arraydev.com/commerce/jibc//
[40] Reserve Bank of India, *Guidelines on National Electronic Funds Transfer System Procedural Guidelines*, April 2011, RESERVE BANK OF INDIA, Department of Payment and Settlement Systems, CO, Mumbai page no.4-12, (21 Dec. 21, 2019, 10:30 AM) http://www.rbi.org.in/commomaman/English/script/faqview.aspx?id=274
[41] *Id*
[42] Reserve Bank of India - Payment and Settlement Systems Rbi.org.in, https://www.rbi.org.in/scripts/PaymentSystems_UM.aspx (last visited June 12, 2021).

printouts or any kind of data stored in discs, floppy, or tape recording or any other kind of electro-magnetic devices where the data can be stored. This section tries to draw a parallel image of written form of recording and electronic form. The printouts or the electronic data should be certified by the bank manager or by a person who is in charge of the computer.[43]

V. TECHNIQUES FOR AVOID ONLINE BANKING FRAUDS IN INDIA

To curb online banking frauds, one is required to understand them in the perspective of technological advancement and the ease with which they can be committed. As far as the law enforcement agencies are concerned, prevention of crime is more important and one of the priority than the detention of one after it has occurred. Collection of intelligence on suspects, surveillance, warning minor offenders are also important aspect of crime prevention. The major concern is that, many of the social norms and ethics, which act as a deterrent to the commission of crime in the real world, are either non-existence or under developed for conduct over internet. Prevention of online baking frauds defiantly need different approach than in the real world.

(a) **Technology as aid to prevention**: High Technology crime (using computer for accessing bank server, or account information of customer) must be prevented using high technology. In cyberspace, Internet browsers can be configured repeated entry attempts for sensitive web sites or could be coded to prevent certain forms of encryption. Encryption is another way by which online banking frauds can be prevented. Encryption is a system or technique that renders a message unintelligible by anyone other than intended recipient of the message. Encryption while being a boon to prevent crime has also the demerit of being used by criminals.

(b) **User Awareness:** Since computers uses for online banking transaction which are easy targeted by criminals, making them aware of security measures is one of the best means of preventing crime on the internet. Security can be protected are- access control through use of secure passwords, cryptographic tools making communication secure, shielding of emission, using firewall technology to screen traffic. Organisations (Bank officials) stand to gain a lot by training their employees in safe practices and threats of security.

(c) **Expert Dedicated to High:** Tech Crime: The complex technical and legal issues raised by computer-related crime especially online banking crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a bank/firm understanding of computers and telecommunications. The complexity of these

[43] § 2, The Bankers Books Evidence Act, 1891.

 [ISSN 2581-5369]

technologies and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and officers to work these cases on full-time basis, immersing themselves in computer-related investigations.

(d) **Regular and Frequent Training:** Because of the speed at which communication technologies and computers evolve, and because criminal methods in these areas generally change more rapidly than those in more traditional area of crime, experts must receive regular and frequent training in the investigation and prosecuting of high-tech online banking fraud cases. Programs such as those offered by the Government agencies with help of private companies (specialised in cyber securities and investigation) under the National Cybercrime Training Partnership provide such training given to bank official, cyber police officers and investigation agencies and local law enforcement personnel.

VI. CONCLUSION

There is no doubt that online banking fraud is serious threat to current techno-world. India has the second largest number of internet user across the globe. Information technology development in banking industry has also led to the increase of cybercrime including online banking fraud in India. With the increase in the number of online banking frauds and related crime, the government come with legislation, Information Technology Act, 2000 along with refined regulations, new IT technology, to protect the interest of consumer and safeguard against the online fraud. To combat online banking frauds banks likely adopt technologies such as mobile, cloud, remote access, and IoT, not out of choice but out of the need to sustain business during the pandemic and thrive thereafter. Such transformative digitisation will also result in an increased attack surface. Banks will have to prioritise and invest in cyber defence to create an agile and resilient infrastructure of the future. Such an infrastructure will address the current cybersecurity risks and prepare itself for cyber challenges of the future. Accelerating cyber capabilities to match the speed of digital transformation will require executive attention, prioritisation, budget, resources, and governance. Banks officials will decide the degree of agility, pace of change in infrastructure, and collaborative efforts required towards building cybersecurity of the future.

*****

 [ISSN 2581-5369]