LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 1 | Issue 2

2023

ANALYSING THE NOTION OF CYBER CRIMES: A LOOMING THREAT TO THE INDIAN E-BANKING SECTOR

Ananya Jain[1]

I. ABSRACT

"*Technological progress is like an axe in the hands of a pathological criminal*".

~Albert Einstein.

Traditionally, banking required a consumer to wait in a long line even to withdraw money or do other auxiliary tasks. The gap between the bank and the customer has shrunk since financial services are now accessible around-the-clock through ATMs, internet banking, transfers through NEFT and RTGS, etc. E-banking includes much more than simply employing computer-based systems for banking. An information and communication technology-based service is internet banking, frequently termed e-banking.

A slightest bounce or carelessness in how we manage our digital lives can invite cybercrime and cause financial loss. We must therefore exercise caution and vigilance whenever we interact with the outside world digitally, whether it be for online gaming, social networking, business, or other purposes. According to the most recent statistics from January 2023, there were approximately 692.0 million active internet users,[2] and this increase has raised the likelihood that a user will fall victim to this malicious sort of crime, which has been on the rise over the previous few decades. When deploying Internet banking and related services, customers constantly fret about the anonymity of their financial information. It is pertinent to demonstrate to Internet banking users about potential risks and how to remain cautious.

[1] Final Year Student, University of Petroleum and Energy Studies (UPES), Dehradun.

[2] Simon Kemp, *Digital 2023: India*, DATAREPORTAL (Feb. 13 2023), https://datareportal.com/reports/digital-2023-india#:~:text=There%20were%20692.0%20million%20internet%20users%20in%20India%20in%20January,at%20the%20start%20of%202023.

The study in this paper examines and assesses the consequences of online banking services in terms of potential cyber vulnerabilities. Moreover, it delivers basic advice on how users can avoid becoming victims of cybercrime as well as an overview of cybercrimes in the e-banking industry.

II. KEYWORDS:

Cybercrime, Financial Fraud, Cyber Security, E-Banking, Identity Theft.

III. INTRODUCTION

India's banks have migrated to core banking platforms and shifted transactions through electronic channels including ATMs, Internet Banking, and Mobile Banking as well as payment cards (debit and credit cards). The banking sector has benefited from modern technology's ability to bring about significant changes, witnessed an expansion of its services, and now aspires to use it to provide greater customer facilities. This is due to the swift development of computer and internet technologies.

Electronic banking, or e-banking, is an avenue of conducting banking activities that rely on information and computer technology rather than human personnel. E-banking is distinct from typical banking services in that there is no direct communication between the bank and its clients. Internet security is more important than ever since cybercrimes are becoming the biggest issue confronting financial institutions in the twenty-first century. One of the foremost shortcomings now confronting the global Internet banking sector is cybercrime.

Organizations need to comprehend the consequences of cybercrimes in order to apply the proper measurements. Financial institutions need to understand the risks associated with the use of the Internet and take all significant precautions to raise public awareness of personal safety and the necessity for a durable economic condition for business. Cybercrimes have impacts that transcend beyond compromising the financial security of financial institutions and other commercial entities. Organizations need to comprehend the consequences of cybercrimes in order to apply the proper measurements.

The modern world now has an information society thanks to the quick development of mobile networks and information technology. Even while this development makes it much simpler for computer users to access information, there are still assured barriers that must be taken into the forefront.

In the contemporary information-technology world with Internet banking services, there is still a concern of losing personal information or being a victim. Security developers employ a variety of strategies to offer safe financial systems. Computer fraudsters and thieves, meanwhile, have made little progress.

It is necessary to take a comprehensive strategy in the battle against computer fraudsters and cyber-terrorists by creating effective legislation and a sound legal framework to safeguard online financial transactions and other activities.

IV. RESEARCH QUESTIONS

1. What are the most frequent cybercrimes committed in the Indian e-banking industry, and what effects do they have on banks, clients, and the broader financial ecosystem?
2. What are the primary e-banking shortcomings in India that render the industry vulnerable to cybercrimes, and how can these e-banking system security issues be resolved?
3. How successful are India's present legal and regulatory frameworks at preventing and managing cybercrimes in the e-banking industry given the constantly shifting nature of cyberthreats?
4. What are the best practices and recommendations for Indian banks in terms of preventing, detecting, and responding to cybercrimes in the e-banking industry, and how can these recommendations be put into effect to improve banks' cybersecurity gestures?

V. REVIEW OF LITERATURE

The current research is both analytical and comprehensive. To conduct research on this issue, a variety of articles and books on the subject in order to grasp better and

interpretation of the subject have been referred. Below is a summary of the papers and books that were referred in the course of this research work:

- **Princess Preet Kaur Kalra, *India: Scams And Frauds: Black Eyes In The Banking Industry*, MONDAQ (Mar. 21, 2022),**

  The article explains how common scams and frauds are in India's banking sector, which has hampered the country's economy and eroded public confidence in the financial system. It emphasises how the banking industry must take a more proactive stance in discovering and combating scams. There are several recommendations on how to combat financial fraud, including putting in place efficient fraud detection and prevention systems, bolstering internal controls, and enhancing employee training programmes.

Overall, the paper emphasises how crucial it is for the banking sector to adopt proactive measures to stop fraud and preserve public confidence in the financial system.

- **Mrs. S. Kalpana and Dr. Mahalakshmi, *Cyber Crime: A Growing Threat to Indian E-Banking Sector*, 7 JETIR Issue 12 (2020).**

The author discussed on how we are adopting information and communication technology more and more in our daily lives and the hazards of cybercrime that may arise. It highlights the significance of practicing caution and vigilance while interacting digitally with the outside world in order to prevent financial loss. An overview of cybercrimes in the world of electronic banking as well as basic advice on how to avoid being a victim of cybercrime is provided. Moreover, it emphasises how operational, credit, and market risks might have an adverse effect on banks' reputations and erode the public's trust in the usage of e-banking channels.

- **Dr. Raju Majhi, *Cyber Crimes in Banking Sector in India: A Critical Analysis*, THE LAW BRIGADE PUBLISHER 113 (2022).**

The author offers a critical examination of cybercrimes in India's banking industry. It highlights how customers are increasingly relying on electronic delivery methods to complete transactions, leaving them open to dangers from cybercrime. The article

discusses numerous cybercrimes that may happen in the banking industry, including ransomware attacks, identity theft, and phishing. The article stresses the necessity for banks to adopt a proactive strategy to identify and prevent cybercrimes and also addresses the legislative framework in place to combat cybercrime in the banking sector.

- **M. R. CHITGOPEKAR AND V. K. KAPOOR, CYBER CRIME AND THE THREAT OF ONLINE BANKING FRAUD (IGI Global 2014).**

This book addresses the different dangers and shortcomings related to Indian electronic payment and banking systems and provides measures for safety of online banking in India. The authors outline some of the most prevalent forms of cybercrime, such as phishing, social engineering, and identity theft, as well as helpful tips for reducing these risks. Additionally, they include case studies of actual attacks on Indian banks and financial institutions to help readers understand the gravity and extent of the issue.

- **M. Shuaib Ahmed, Akshayaa M R and Dr. N. Gopinathan, *Cyber Law Vis-À-Vis Net Banking in Indian Sector*, SSRN (2021).**

The authors discuss about how E-Banking has grown in India and how net banking has streamlined banking processes. The growth of E-banking may be hampered by concerns about online fraud and cybercrime, though. The paper investigated many instances in which electronic banking has been in danger and also provides a history and development of electronic commerce in India. Some countermeasures to potential risks in the e-banking industry are provided at the end.

- **Vihang Dilip Gaokar,Karan Harish Tundejwala, Cyber Crime in Online Banking, 7 IJARSAT Issue 1 (2021).**

The article discusses the importance of protecting privacy in the digital age, especially in the context of online banking transactions. It highlights the increasing threat of cybercrime and the ease with which hackers can manipulate victims to steal their money. The author stresses the need for greater awareness of cybersecurity and the potential risks associated with online banking. The article concludes by emphasizing

the significance of protecting data and finances in the banking sector, given the rising instances of online fraud and financial losses.

VI. CONCEPT OF E-BANKING IN INDIA

The act of utilizing an online platform as a remote delivery channel for financial services, such as opening a deposit account or moving money between accounts, is known as Internet banking. Online banking use is expanding and evolving.[3]

E-banking stands distinct from traditional banking services in that there is no direct connection between the bank and its clients. Through an abundance of platforms that may be connected to a variety of terminal devices, such as a personal computer and a mobile phone with browser or desktop software, telephone, or digital television, banks can give information and services to their clients.[4]

A web page, which is the cornerstone of Internet banking, must first be created by a bank in order to provide information about its offerings. Providing facilities like account access, money transfers, integrated sales of other operations, and exposure to other financial services including investing and insurance are all included at a higher level. Internet banking provides access to a variety of services, including online share trading, online money transfers, electronic bill payment systems, train bookings, money transfers from one customer's account to another, loan applications, and more.

Internet banking has three functional levels: informational, communicative, and transactional.

Banks have been found to have marketing materials about their services and goods on an independent server, based on the extent of the information. The degree of communication in internet banking enables certain client and bank system engagement. Transactional-level Internet banking allows bank clients to electronically

[3] *Internet Banking*, CASHLESS INDIA (accessed on Apr. 21, 2023), http://cashlessindia.gov.in/internet_banking.html.
[4] Ms. Neeta and Dr. V.K.Bakshi, *Cyber Crimes In Banking Sector*, 6 AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (AIRJ) 25 (2019).

transfer funds to and from their accounts, pay bills, and conduct other financial transactions online.[5]

VII. CYBER CRIME IN E-BANKING IN INDIA

Any illegal behaviour conducted online or through a computer is indicated as cybercrime. Digital misbehaviour is sometimes referred to as "cybercrime," when a perpetrator uses the internet and other electronic devices with improper authorization to perform a variety of acts of violence, including money transfers and withdrawals.

Internet banking and credit card services are only two of the many services that the banking industry offers to its clients and consumers, to help condense the landscape in today's globalized world. In online debit card payments, customers may simply transact and manage their accounts via the internet and mobile devices from anywhere in the world, and they have access to all sorts of bank services 24 hours a day.[6] As everyone seems to know, these services provide advantages to consumers, but they also have drawbacks like hacking and theft.

Cyber terrorism, cyberbullying, computer vandalism, software piracy, identity theft, online theft and fraud, email spam and phishing are only a few examples of the numerous segments that cybercrimes may be generally categorized into. But when it comes to electronically committed financial cybercrimes, the following types predominate:

- **Hacking** is a technique for gaining unauthorized access to a computer network or system in order to steal, corrupt, or view data improperly.
- The practice of "**phishing**" involves pretending to be a reliable person in an electronic contact in order to get sensitive data, such as usernames, passwords, and debit/credit card details, which is subsequently used for illegal activities.

[5] Dr. Vijayalakshmi, Dr.V.Priyadarshini, Dr. Umamaheswari, *Impacts Of Cyber Crime On Internet Banking*, 2 INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY AND MANAGEMENT SCIENCES 30 (2021).
[6] A.R. Raghavan and Latha Parthiban, *The Effect of Cybercrime on a Bank's Finances,* 2(2) INTERNATIONAL JOURNAL CURRENT RESEARCH ACADEMIC REVIEW 173 (2014).

- **Vishing** is the name given to the illegal activity of utilizing social engineering over the phone to get people's private information and sensitive financial information in order to generate money.
- **E-mail spoofing** is the process of altering the email header to make it seem as if it came from a reliable source rather than the actual source from which it originated.
- **Spamming** is the act of sending many, undesired, and un-subscribed emails to those who would not ordinarily wish to receive them.
- **Denial of Service:** The act consists of an overt attempt by attackers to prohibit authorized users of a service from utilizing that service. Attackers may try to do this via "flooding" a network to block allowed network traffic, interfering with connections between two computers to limit access to a service, or preventing a particular user from utilizing a service.
- **Advanced Persistent Threat**: It is characterized as a group of complex, stealthy, and persistent computer hacking methods that often focus on a single target in order to gain unauthorized access to a network and gather sensitive data over a prolonged period of time. The attacker often makes use of social engineering to access the targeted network through legitimate means.[7]
- **ATM Skimming and theft at the point of sale**: By adding a skimming device to the card reader or ATM keypad and making it seem as if it is a legitimate keypad or an essential part of the machine, it is possible to hack POS systems or ATM machines. Additionally, these devices can have malware installed that specifically gathers credit card information. Skimmers utilize ATM card readers to collect card numbers and personal identification numbers (PIN), which are then copied to conduct unauthorized transactions.[8]

[7] Seema Goel, *Cyber-Crime: A Growing Threat To Indianbanking Sector*, 5 INTERNATIONAL JOURNAL OF SCIENCE TECHNOLOGY AND MANAGEMENT 552 (2016).
[8] *Id.*

- **Impersonation and identity theft** are crimes that include using another person's electronic signature, password, or other distinctive feature without that person's permission or knowledge.
- **Fraudulent use of a Google Pay, PhonePe, or Paytm QR code or link**: Cybercriminals email their victims debit links or QR codes that may be scanned to make deposits into their bank accounts using Google Pay, PhonePe, or Paytm. However, when scammers send a link or QR code demanding money, the victim's money really vanishes from their account without ever being received.
- **Social Engineering**: Social engineering is the process of getting others to do our duties or divulge private information. Social engineering is a branch of social science that is often used by online criminals and computer fraudsters to get sensitive data and financial information.[9]
- **Social Networks:** Social networking services provide online impersonators access to information posted by account users. Data that has been taken by cybercriminals may subsequently be used for illicit activities. Scammers may use links to send users of these social media sites, such those on Facebook and Twitter, to another website so they can connect quickly.
- **Mobile Phones and Electronic Devices**: In today's digital era, using mobile phones and other electronic devices like computer tablets has become normal. Users of smartphones and tablet computers are in grave risk from hackers and computer thieves, according to security specialists.[10]
- **Electronic media platforms**: Nowadays, people use increasingly advanced browser-enabled technology at home. These include devices for streaming media and "smart" TVs from a variety of manufacturers that are linked to the internet. Nearby is a Google TV illustration. Customers are concerned about their security while using these services to access the internet. Through

[9] *Supra* Note 4.
[10] *Supra* Note 4.

regulated apps, the platforms make it simpler for scammers and hackers to manage a range of physical equipment.[11]

VIII. IMPACT OF CYBER CRIMES IN BANK FINANCES

Cybercrime incidents have sharply risen as mobile devices with internet connections have proliferated. Given that they are used for a range of online activities, such as online banking, shopping, and paying utility bills, smartphones are often targeted by hackers aiming to steal private data in the current day. Over the last several years, monetary gain has consistently outpaced other reasons, such as vengeance, extortion, and political objectives, as the primary cause of cybercrime.

Unfavourably, simple phishing efforts have a strike rate of 45% due to ignorance of the typical safeguards against smart hackers.[12]

Internet banking transactions are far less expensive than traditional banking operations. Because setting up Internet banking is less expensive for banks, several new trends are being introduced in the banking industry as a result. The traditional banking system may find it difficult to raise more cash or make investments in the stock markets, in contrast to the internet banking system, which seems to be a very simple task to connect with.

Internet banking is becoming a vital part of the global financial industry since it can meet the needs of different financial markets and businesses. With the increase in global internet users, online banking has become more popular and has a huge impact on both local and global economies.

IX. CYBER ATTACKS IN INDIA

- **Cosmos Bank Cyber Attack in Pune:**

Hackers stole money from Pune's Cosmos Cooperative Bank Ltd., totalling Rs. 94.42 crores, shattering the whole banking sector in India. Cosmos Bank in Pune was the subject of a recent hack in 2018. Using the bank's ATM server access, hackers acquired a significant amount of personal information from users of Visa and Rupee debit

[11] *Supra* Note 4.
[12] *Supra* Note 4.

cards. Hacker groups from as many as 28 countries immediately withdrew the money after being informed that it had been lost. It may be prevented by stepping up surveillance processes and supporting authorized people.[13]

- **ATM System Hacked:**

The Canara Bank ATM servers were the subject of a breach in 2018. Many different bank accounts saw the clearing of twenty lakh rupees. 50 individuals were reportedly impacted altogether as a consequence of hackers having access to more than 300 people's ATM information, according to sources. Hackers utilized skimmer devices to steal debit cardholder information. The value of transactions including stolen data ranges from Rs. 10,000 to Rs. 40,000. If the security features in ATMs are strengthened, data abuse might be prevented.[14]

- **RBI Phishing Scam:**

The hackers' audacious phishing effort included the Reserve Bank of India. The receiver of the phishing email, which claimed to be from the RBI, would be promised Rs. 10 lakhs in prize money within 48 hours if they clicked on a link that led them to a website that looked just like the RBI's official website—complete with the identical logo and web address. The user is then asked for personal information, such as their password, I-pin, and savings account number. On its official website, the RBI, on the other hand, issued a warning on the false phishing email.[15]

- **The NSP Bank Case**

A bank management trainee was hired. They communicated with each other through email on the company's PCs. After their breakup, the girl used many fictitious email addresses, including "Indian bar associations," to communicate with the boy's overseas clientele. On the bank's computer, she completed this. The boy's company

[13] Express News Service, *Cosmos Bank Malware Attack: Interpol Issues Red Corner Notice Against Prime Suspect Traced in Foreign Country,* INDIAN EXPRESS (Aug. 29, 2020) https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-interpol-issues-red-corner-notice-against-prime-suspect-traced-in-foreign-country-6574097/.
[14] Ranjitha S, *4 Biggest Cyber Security Threats for Indian Banking Sector*, GREAT LEARNING (Mar. 24, 2021), https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-banking-sector/#:~:text=Canara%20Bank%20ATM%20servers%20were,rupees%20from%20various%20bank%20accounts.
[15] Vivek Kumar Verma, *Phishing,* INDIAN CASE LAW (July 16, 2014), https://indiancaselaw.in/phishing/.

suffered significant customer losses and therefore sued the bank. Since the emails were transmitted utilizing the bank's infrastructure, the court decided to hold the bank accountable.[16]

The above-mentioned assaults in India should serve as a warning to all individuals and organizations that are already exposed to cyber dangers. The banking industry and its businesses must employ cyber security measures and comply to security regulations.[17]

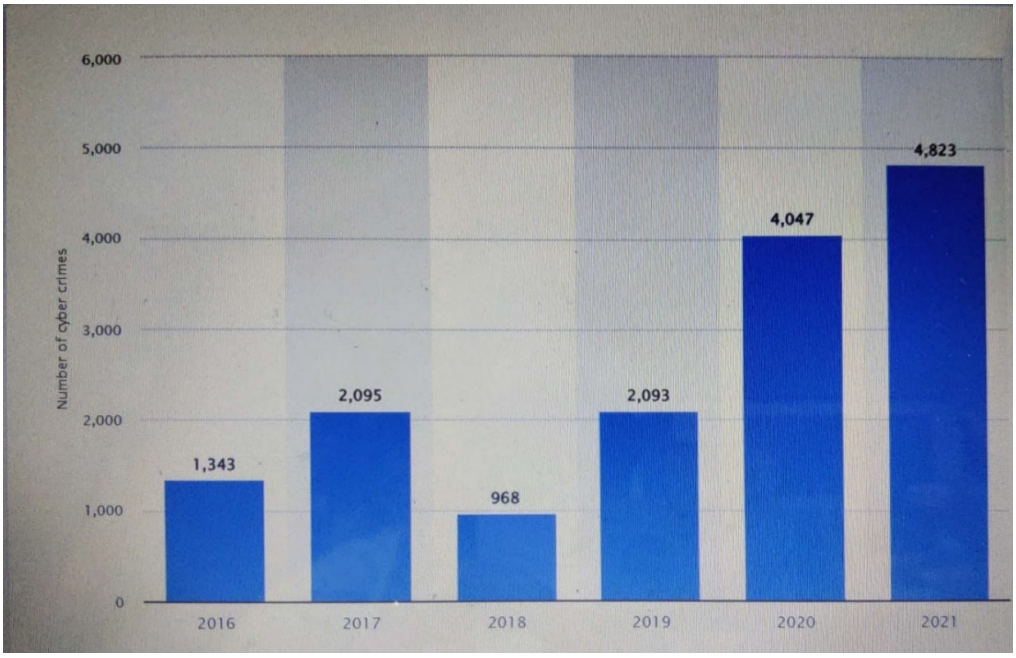
- **India's First ATM Card Fraud**

The Chennai police have captured an internet criminal group. 22-year-old Deepak Prem Manwani was detained by the police after being charged with stealing an ATM in June. When he was apprehended, the police said that he was carrying Rs 7.5 lakh that he had stolen from two ATMs in The Nagar and Abirami Puram neighbourhoods of Chennai. Before departing, he had already taken out Rs 50,000 from an ATM in Mumbai.

After withdrawing from an MBA program in Pune, Manwani was employed by a corporation with headquarters in Chennai. He used to get credit cards from a few American banks from some buddies in Europe for $5 each. The administrator of the website in Europe devised a cunning plan to get the distinctive ID numbers of the users. After receiving a significant number of complaints from charged Visa users and banks in the US, the FEI opened an investigation and informed the CBI in New Delhi that the universal pack had also increased in India.[18]

[16] Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah, *A brief study on Cyber Crime and Cyber Laws of India* 4(6) IRJET 1636 (2017).
[17] Himanshi Lodha and Divya Mehta, *An Overview of Cyber Crimes In Banking Sector*, LEGAL SERVICE INDIA (accessed on Apr. 21, 2023), https://www.legalserviceindia.com/legal/article-7694-an-overview-of-cyber-crimes-in-banking-sector.html.
[18] CA Mayur Joshi, *ATM Frauds in India evolved during digitization*, INDIA FORENSIC (accessed on Apr. 21, 2023), https://indiaforensic.com/atmfraud.htm#:~:text=Meanwhile%2C%20Manwani%20also%20managed%20to,lookout%20for%20those%20persons%20too.

X. RECENT STATISTICS OF CYBER CRIMES IN INDIAN E BANKING SECTOR



Over 4.8 thousand instances of internet banking fraud were recorded in India in 2021. Telangana recorded the most instances of financial fraud that year, totalling roughly 2,180.[19]

A. SECURITY MEASURES:

Customers of digital banking must be informed of the most basic security procedures to prevent cyber-attacks and protect their financial data.

i. **Secure the gadgets:** At first, there are severe concerns about the security of the equipment used to access Internet banking. These gadgets include computers, mobile devices, and other tools for accessing Internet banking.

ii. **Secure your personal information:** Security of data is crucial. Personal information and confidential information should not be shared with

[19] Tanushree Basuroy, Number of cyber crimes related to online banking across India 2016-2021, STATISTA (Oct. 14, 2022), https://www.statista.com/statistics/875887/india-number-of-cyber-crimes-related-to-online-banking/.

everyone. When sharing information, it's important to keep the intended audience in mind and take additional precautions to prevent social engineering or other tactics employed by cyber-criminals and computer fraudsters. Customers of online banking must understand how to encrypt data used by financial organizations, such as banks, and for tax returns.

iii. **Establish Strong Passwords:** Internet banking users are usually urged to use strong passwords. Computer thieves may use a range of tools to decrypt or guess consumers' Internet banking credentials. Furthermore, it is advised that passwords not be recorded anywhere. For a strong password, you should utilize combinations of various alphabets, numbers, and special characters.

iv. **Be Responsible Online**: When transacting online, personal information must be kept private. Every social media account has to be turned to private. Social media accounts' security settings should be periodically examined. One shouldn't disclose sensitive or private information on social networking.

v. **Install and upgrade System and Software:** It is suggested that Internet users update their systems and software to avoid security breaches.

XI. LEGAL FRAMEWORK OF INTERNET BANKING IN INDIA

The Reserve Bank of India Act, 1934 and the Banking Regulation Act, 1949 both play a significant regulatory role in Indian banking. The Information and Technology Act, 2000, as revised in 2008, governs electronic records and systems. Internet banking is only the practice of doing business through electronic channels, and it is merely one more service offered by the banks. In India, there are several laws that regulate online banking. These laws include the Indian Contract Act of 1872, the Banking Regulation

Act of 1949, the Information Technology Act of 2000, and others. Let's examine the provisions of all these significant financial laws. [20]

1. Information Technology Act, 2000

The Information Technology Act, 2000 is India's principal statute addressing electronic commerce and cybercrime. It may thus be claimed that Internet banking cannot be conducted without complying with the IT statute 2000 since this statute directly affects how internet banking functions in India.

The following details emphasize the significance of the Information Technology Act of 2000 in relation to online banking:

i. Document scrutiny: Any financial transaction requires the scrutiny and preservation of a number of papers. In online banking, these documents are preserved and examined digitally. Only the IT Act provides these electronic papers with legal validity.[21]

ii. Electronic Transaction: The provisions of the IT Act recognize any transaction entered electronically. Since Section 10-A of the Act provides an electronic transaction legitimacy and enforceability, no online banking transaction may be challenged in court without the requirements of the IT Act.[22]

iii. Authentication**:** These electronic records should be authenticated in accordance with the provisions of this act in order to be used for electronic banking.

iv. Digital Signature: If the papers are signed digitally or electronically, only this act's requirements apply. Therefore, for the purposes of Internet Banking, this action would fulfill the requirement of signing a document.

v. Privacy: Privacy is crucial for online banking since without privacy and security, it's possible that the industry wouldn't have lasted.[23]

[20] Rohit Jain, *Legal Framework of Internet Banking in India*, 4 INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES 699 (2021).
[21] Information Technology Act 2000, Chapter III.
[22] Information Technology Act 2000 § 10-A.
[23] Information Technology Act 2000 § 72.

vi. Data theft: According to Section 66 of the IT Act, a range of activities involving theft from computer systems are punishable. A few examples of such acts include hacking, the introduction and dissemination of viruses over computer networks, and others.

vii. The goal of the IT Act is to make e-commerce and e-government easier to use, both of which are crucial for Internet banking in India.

The Information Technology Act, 2000 has created the key legal framework required for Indian Internet banking, according to an analysis of the aforementioned difficulties. Consequently, a comprehensive strategy must be used to create consistency and harmony between the IT act's standards and the Reserve Bank of India's published directions.

The following are a few of the key provisions of the IT Act:-

a) Section 3(2)[24]: The crypto function and hash function are the only methods of electronic record authentication acknowledged in this section. Different countries have maintained the technology-neutrality of this strategy.

b) Section 4[25]: This section governs the legal recognition of all contracts and agreements made in electronic form.

c) Section 72[26]: It specifies the punishment in the event of a privacy infringement.

d) Section 79[27]: This provision shields network service providers from legal responsibility for any criminal behavior carried out through their network.

The G Gopalakrishna Working Group was created by the RBI in January 2011 to look into the safety of electronic banking in India. In April 2011, the committee made a few changes to the current regulatory standards.[28]

2. Indian Penal Code, 1860

[24] Information Technology Act 2000 § 3, cl. 2.
[25] Information Technology Act 2000 § 4.
[26] Information Technology Act 2000 § 72.
[27] Information Technology Act 2000 § 79.
[28] *Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds Report and Recommendations*, RESERVE BANK OF INDIA MUMBAI (Jan., 2011), https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf.

The Indian Penal Code contains penalties for a number of offenses using Internet banking. The IPC contains a number of regulations that guard against theft, fraud, and other crimes relating to Internet banking. Unsurprisingly, the IT Act, 2000 and the Indian Penal Code have a number of sections. Here are a few of such clauses in more detail:

- The term theft under Section 378 of the IPC includes online and offline data theft. Information pertaining to online banking might be taken in a number of methods, including hacking, virus propagation, computer system exploitation, and denying access to someone who should have it. As a consequence, data protection becomes crucial. To protect the interests of users of online banking, IPC also forbids such behaviour. Section 424[29] of the Indian Penal Code forbids data theft and punishes those who assist or conceal the theft.
- Receipt of stolen items: Under Section 411[30] of the IPC, anyone found in possession of goods purchased via an internet banking transaction is guilty of the crime and is subject to a maximum three-month prison term, a fine, or both. The IT Act's Section 66-B[31], which imposes penalties for dishonestly acquiring stolen computer resources or communication devices, is analogous to this section of the IPC.
- Personation Cheating: Any conduct performed by personation cheating is punishable under IPC Section 411 (Dishonestly accepting Stolen Property). The same is punishable under Section 66-C[32] of the IT Act. Cheating by Personation is the term used to describe someone who violates the law by using a computer to cheat.
- Mischief: It should go without saying that anyone who knowingly introduces viruses into a computer system, harms the system, or prevents someone who is authorized to use it from accessing it is guilty of mischief and is subject to up to three months in jail, a fine, or both under Section 425[33] of the IPC.

[29] Indian Penal Code 1860 § 424.
[30] Indian Penal Code 1860 § 411.
[31] Information Technology Act 2000 § 66-B.
[32] Information Technology Act 2000 § 66-C.
[33] Indian Penal Code 1860 § 425.

- Forgery: Fraudulent electronic documents or other information may be sent during online banking transactions.[34]

The IT Act has penalties for a variety of additional criminal offenses that the IPC does not address. Most of them are not:

- A person who uses any computer system, computer network, or other device to tamper with or manipulate is not punished under the IPC for doing so. Such behaviour is prohibited under Section 43(h) of the IT Act.
- Modifying the source document on the computer. Section 409 of the IPC partly punishes it, however it doesn't specify the penalty in great detail. As a result, section 65 of the IT Act applies.
- Online security or privacy violations are punishable under Section 66E of the IT Act.
- In Internet banking, privacy is crucial while signing in, inputting a password, and conducting transactions.
- Preservation of Intermediaries: Section 67 requires that a "intermediary" preserve and hold onto all required information. In our case, it would be banks. In the case of *Shreya Singhal v. UOI*[35], when this clause was contested before the court, the court upheld the section's legality.

3. **Other Legislations**

    - **INCOME TAX ACT, 1961: Section 40A (3)**[36] **-** The account holder only benefits from this part when money is transferred by cheque or internet banking. This section tries to prevent tax avoidance by requiring the bank to closely monitor any transactions totalling more than $20,000.
    - **NEGOTIABLE INSTRUMENT ACT, 1881**: **Section 6**[37] included the ideas of a truncated check and an electronic check. These checks are electronic negotiable instruments that are a feature of online banking. By

[34] Indian Penal Code 1860 § 468.
[35] (2013) 12 S.C.C. 73.
[36] Income Tax Act 1961 § 40A, cl. 3.
[37] Negotiable Instrument Act 1881 § 6.

using digital signatures (which might be connected to biometrics), all of these equipment's must uphold certain minimal safety standards.

- **PREVENTION OF MONEY LAUNDERING ACT, 2002**: **Section 11**[38] mandates that all intermediaries and financial institutions maintain records of each transaction. All banks, whether they provide services physically or online, are subject to this. This provision helps to prevent money laundering via internet banking.
- **CONSUMER PROTECTION ACT, 1986**: The goals of this statute are to protect consumer interests. Additionally, this also applies to financial services. This law protects issues with internet banking, such as privacy, the secrecy of client accounts, and the duties and rights of both customers and banks.

METHODS TO PREVENT CYBER CRIME

- The banking industry has seen an alarming increase in crimes, which has resulted in significant financial losses. Since banks are the main economic backbone of our society, they must be protected from cyberattacks. Customers and banks should be made aware of the danger and the security precautions to thwart the cyberattack.
- The government has formed a "Inter-Departmental Information Security Task Force (ISTF)" as the focal entity for the efficient execution of all issues relevant to cyber security policy. The Indian Computer Emergency Response Team (CERT-In), the country's nodal organization, is tasked with monitoring computer security problems as they arise.[39]
- Jurisdiction is the major issue with cybercrime. No matter where they reside, everyone should be able to identify and keep an eye out for cybercrime as it occurs in every state. For a number of reasons, including living in a remote place, not knowing where to report, and privacy concerns, victims of

[38] Prevention of Money Laundering Act 2001 § 11.
[39] Harshita Singh Rao, *Cyber Crime in Banking Sector*, 7(1) INTERNATIONAL JOURNAL OF RESEARCH - GRANTHAALAYAH 158 (2019).

cybercrime may be unable to file a complaint. Because there is no centralized way for monitoring them, many incidents of online crimes go undetected.[40]

- A definition of cybercrime and a list of circumstances in which the IT Act would have extraterritorial power should be added to the current text of the law. The IT Act need to provide India's internet activities with a legal structure. The obligations of the intermediaries need to be made clear, although they are not always clear.

Here are few strategies to lessen the risk of a cyber-attack: [41]

- Every employee has to have a user account, and there should be a rule mandating password changes every three months. Unauthorized software cannot be downloaded or installed by employees.
- It is necessary to inform all staff members of the risks involved in downloading or opening email attachments from untrusted sources. Inform staff members of the value of keeping confidential information about the institution to themselves.
- Every workstation and Internet-connected gadget in the bank's IT department has to have a firewall set since it prevents all contact from untrusted sources.
- Wherever practicable, banks must establish "two-factor authentication" (2FA) on all online accounts using applications or physical security keys.
- All PC operating systems will get routine security upgrades thanks to the Department.
- All PCs must possess anti-virus and anti-spyware software running in order to check for the presence of ransomware or other harmful malware on the network. Wireless networks and all passwords need to be kept safe and protected.

[40] *Id.*
[41] *How the Banking Sector Can Combat Cyber Attacks: A Checklist*, BYTE ACADEMY (Aug. 6, 2020), https://www.byteacademy.co/blog/banking-cyber-security.

- Banks must implement verification methods including dynamic device authentication and web-based transaction verification as more clients use mobile devices.
- Banks must notify customers and send them automated communications verifying the accuracy of their transactions.
- Customers must be provided with information on how to confirm the reliability of any parties requesting personal account information. Additionally, clients must get guidance on how to properly access the bank's websites.
- Use a secure network while utilizing a banking application or online banking.

XII. OBLIGATIONS OF BANKS

There are a few requirements that any financial institution must adhere to:

1. **Duty to maintain Customer Account Secrecy**: In the *Tournier's Case, 1924*[42], it was decided that bankers have a responsibility to adhere to Customer Account Secrecy. The nature and specifics of the accounts never be revealed to anyone as it could affect the customer's prestige and creditworthiness. Due to the existence of hackers, this task has now become more challenging due to the expanding field of online banking and the rising threats of cybercrime.
2. **Obligation to furnish documents to courts**: It is the banker's responsibility to present any documents requested by the court. This is essentially an exemption to the previously stated confidentiality principle. Anytime the court requests the records, the banker must provide them; this does not violate anyone's privacy.[43]
3. **The responsibility to confirm the legality of a digital signature**: One must comply with in order to the steps outlined in the IT Act of 2000. The paying bank must check the authenticity of the signatures since the law is particularly tough when it comes to falsified documents.

[42] Tournier v. National Provincial & Union Bank of England, (1924), K.B., 461.
[43] The Bankers' Book Evidence Act 1891 § 4.

4. **The need to provide services to customers**: Banking institutions are required to provide a range of services to their clients (some of which are covered in the section below). These services must be made available to online banking customers as well by the bank. In the case of *Vimal Chandra Grover v. Bank of India*, the Supreme Court had previously made the same declaration.[44]

XIII. HOW TO REPORT AND WHERE TO FILE COMPLAINT

The possibility of financial scams cannot be overlooked as the digital world expands, particularly when it comes to banking transactions. Phishing, email spoofing, or card cloning are all examples of fraudulent online transactions that may have included a person's bank account, debit card, or credit card.

You must file a complaint if there is an online transaction fraud involving net banking, ATM transactions, or any other online transaction. However, the victim must have the following documents before submitting a formal complaint to the bank or the card issuer:[45]

- A six-month bank statement from the appropriate institution.
- Make a copy of any SMS messages you received about the purported transactions.
- Make a copy of your identification and your proof of address as they are shown in your bank's records.
- Send the aforementioned papers and a complaint detailing the whole incident to the closest police station. A direct complaint may be filed to the magistrate if any police officer fails to file a FIR.

In the online space, there are many fake programs being distributed. Provide the screenshot of the infected software and the URL where it was downloaded if financial fraud was carried out via an app in addition to the documents stated above.

[44] AIR 2000 SC 2181.
[45] Darshnik Narang, *Cyber Frauds In The Indian Banking Industry*, LEGAL SERVICE INDIA (accessed on Apr. 21, 2023), https://www.legalserviceindia.com/legal/article-3073-cyber-frauds-in-the-indian-banking-industry.html.

- Complaint to RBI - If the concerned bank claims that it won't reverse an unauthorized transaction after you have reported it within the allotted time limit, you may file a complaint with RBI. If your bank refuses to assist with unapproved fraud transactions.[46]

Additionally, the victim can file the complaint online as well.[47] the Indian government launched an exclusive online portal to deal with accusations of cybercrime. The victim can report any cyber-fraud to the National Cyber Crime Reporting Portal.[48]

XIV. FINDINGS AND SUGGESTIONS

Findings:

- Hacking and identity theft have been the main causes of cybercrimes in this field.
- Banks are often the target of assaults since they contain all of the reserves in cash.
- Over the last four years, the cyber cell has handled consistently few cases, with an accomplishment rate of just 20%.[49]
- It has been noted that 50% of respondents strongly agree with taking precautions to backup essential data.[50]
- The software that can be utilized for identifying frauds in the majority of instances is either outdated or excessively time consuming.

Suggestions:

[46] *Complaints*, RESERVE BANK OF INDIA (accessed on Apr. 21, 2023), https://www.rbi.org.in/Scripts/Complaints.aspx.
[47] Divya Bhati, Cyber fraud incidents rising in India: how to file a complaint online on Cyber Crime portal, INDIA TODAY (Feb. 15, 2023), https://www.indiatoday.in/technology/features/story/cyber-fraud-incidents-rising-in-india-how-to-file-a-complaint-online-on-cyber-crime-portal-2335149-2023-02-15.
[48] *Filing a Complaint*, NATIONAL CYBER CRIME REPORTING PORTAL (accessed on Apr. 21, 2023), https://cybercrime.gov.in/.
[49] N. Rexha, R. P. J. Kingshott and A. Shang Aw, *The impact of the relational plan on adopting of electronic banking*, 17(1) COMMUNICATIONS AND NETWORK 53 (2014).
[50] Dr. A. Thilaha Dharmarajan and U. Ezhilarasi, *Cyber Crimes in Banking Sector - An Evaluation*, 1(2) AHALIA INTERNATIONAL JOURNAL OF ADVANCED SCIENCE AND TECHNOLOGY 10 (2021).

- Internet banking customers have to create secure passwords and unique user names for each of their accounts and websites.
- Law enforcement should be especially tough and updated often to maintain track of such infractions.
- In order to settle these conflicts, address public concerns, and promote public confidence, fast-track mobile courts should be formed.
- Using Big Data Banks, the government should also keep an eye on operational network activities.
- To lessen the effects of these problems and punish the perpetrators, a systematic application of punishments and penalties is required.
- To keep client accounts secure, it is advised that all transactions use two-step authentication. It is essential to use updated antivirus software to protect against virus assaults and to preserve backups of important data to prevent data loss in the event of a virus threat.
- Additionally, the bank is urged to implement training and orientation initiatives for bank personnel. It is important to inform employers about fraud protection techniques.
- If rewarded, workers who go above and beyond the call of duty to stop cyber-frauds will increase their commitment to their employment. Bank scams also demonstrate that online banking users are not vigilant and are not sufficiently informed about cyber-threats. Banks possess a duty and obligation to periodically inform and educate their clients about the dangers that are currently facing the industry.

XV. CONCLUSION

Victims should notify the local police station and the bank's cyber fraud committee about these incidents since cybercrime is a more serious offense than traditional crimes. The Indian banking sector cannot escape electronic banking operations in the present climate. To eradicate these issues, lawmakers should rigorously monitor how

banks function, laws that forbid such wrongdoings should be properly implemented, and banks should often educate their customers about cybercrime awareness.

Unaware customers are easily misled because they are unaware of the most recent attack tactics and known preventative measures. Engaging competent cyber security experts takes producing faster and better cybercrime investigation results one step further. India anticipates requiring 1 million qualified Cyber security Professionals by 2025, according to NASSCOM's Cyber Security Task Force.[51]

The legislation regulating online banking in India is inadequate and vulnerable since it hasn't kept up with technological advancements. The challenges of online banking in India include determining the jurisdiction, supervisory controls, security measures, authenticity concerns, recording and proving evidence, etc. The one worthwhile phenomenon about the legislative framework surrounding Internet banking is that the Central Bank, Parliament, and a few other institutions are working hard to create comprehensive law relating to online banking that complies with international standards. And thus, as an observation, it is reasonable to state that India urgently needs to adopt Internet banking laws.

[51] *Cyber Security Task Force*, DSCI (accessed on Apr. 21, 2023), https://www.dsci.in/content/cyber-security/cyber-security-task-force#:~:text=The%20vision%20of%20the%20Task,from%20India'%3B%20thus%20making%20India.