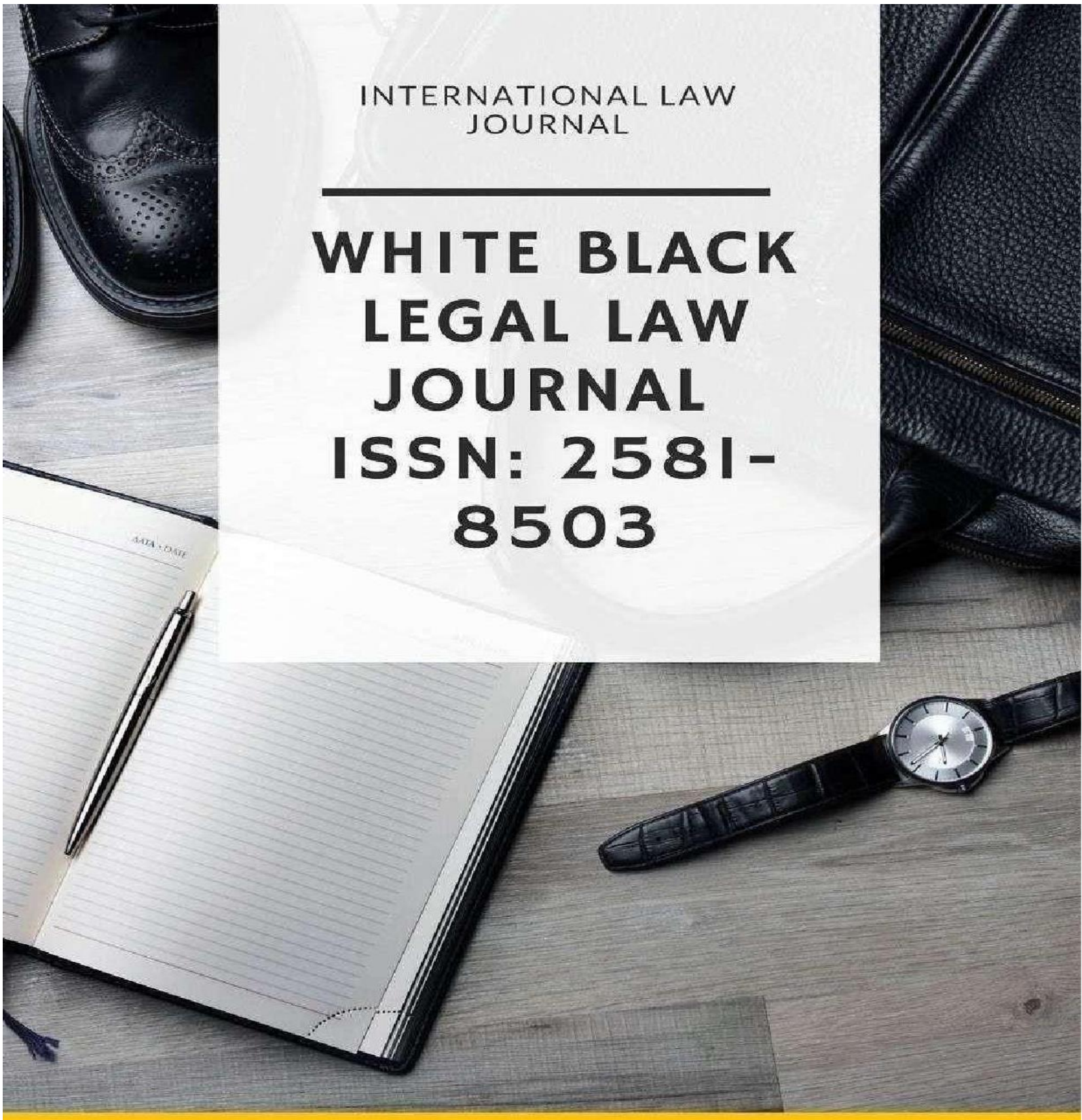


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

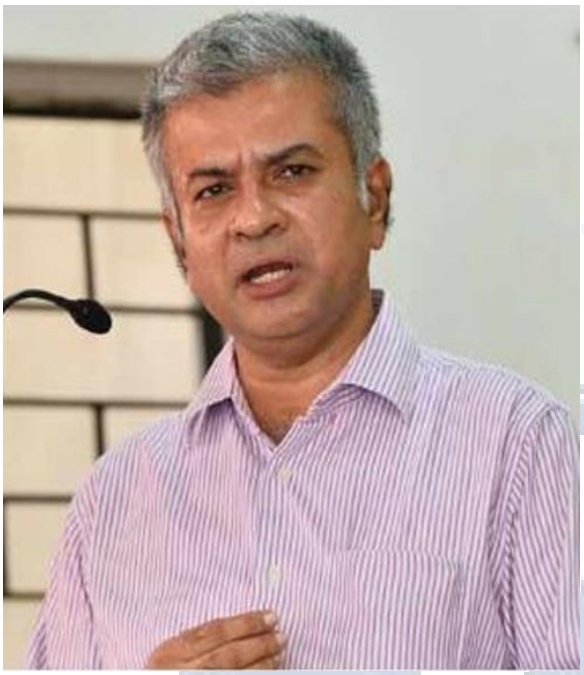
The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

Data Privacy And Digital Transaction -

A Long Walk To Secure Banking

Authored By - Dayem Mohammad Ansari

Affiliation: Student, 3rd Semester LLM,

Govt. Centre of Legal Education, (Hooghly Mohsin College, under the University of Burdwan), &

Advocate (Criminal),

The Calcutta High Court.

E-Mail: dayemansari68@gmail.com

Contact No:8777834566

Postal Address: Q-596/E, (First Floor), Gulab Rab Lane,

Opposite: Sir Syed Ahmed F P School,

Garden Reach, Kolkata-700024.

Declaration:

I do hereby declare that my research paper entitled "Data Privacy and Digital Transaction-A Long Walk to Secure Banking", is an original and unpublished work of mine. I am its single author. All relevant supplements have been duly mentioned along with their sources and this work of mine doesn't infringe any copyright law.

-

ABSTRACT

Keywords: Digital Transaction, Data Privacy, Online Banking, Cyber-Attack. Financial Fraud, Figital (Financial and Digital) Literacy.

With the advancement of science and technology, almost all the major spheres of human activities have gone through a series of drastic changes that not only influenced our lives in best possible ways but also brought many disasters with it as well. The Indian Banking Sector, an age-old institution, too could not keep itself stay away from the course of change and probably, now the banking sector is one of those very few sectors who have been greatly hit by the advent of technology. On the one hand, where doing the banking transactions and business has become very smooth and hassle free, it is also surrounded by the Hydra of various kind of cyber-crime (such as Phishing) that have posed serious threat and imminent danger to the digital banking activities which keeps itself expanding every day. The sharp rise in the number of customers along with digital literacy has not only taught our young generation the effective use of Mobile Phones for making digital payment and other financial tasks but also made the Online Banking System a soft target for cyber-crime which also results in the serious breach of our Data Privacy. In the recent times, when the Lock Down period is over but the threat of Covid still exists, we have seen that cyber-attacks are on all-time high. Though the Central Government and the RBI have made certain legislations and issued various regulations in combating this digital crime, yet we are still far away from securing our Banking Sectors from all malpractices.

In my paper, it will be my endeavour to take a holistic view of the challenges faced by our banking sector along with the issue of Data Privacy which is interrelated with this and what laws/regulations are there for tackling with such menace and what are the road ahead for us while facing such grave challenges, so that it may help general public to understand the interconnection of law and technology and its positive and negative impacts on our daily life.

****

Introduction:

In this revolutionary era of modernization and digitization, the banking system is no longer confined to the arena of simple monetary transactions which were used to done at some small-scale branches with people standing in the queue and holding torn passbooks in their hands. It has gone much beyond the dusty and bulky accounting registers and the old styled gentlemen whose expertise used to lie in counting and calculation only. With the beginning of the twenty first century, the banking and finance sector of India has not only adapted various new measures of transacting the business, but also witnessed a sharp rise in the number of the customers. Moreover, the term 'Banking' is no longer confined to simple money depositing in the savings account, but includes bank guarantee, credit cards, funds remittance, collecting and paying the credit instruments etc. And as we have entered the second decade of this century, despite its modern amenities and digital features, our banking system has many bugs to be fixed which we will discuss in this paper.

Going Digital from Traditional-A brief view:

To put it simply, by digital banking system we mean the system which has replaced the manual banking business with online and digital transaction and as a result, not only has it seen an increase in the efficiency of banking process and services, but also a growth in customers' list as well. A cursory look at our banking system will make us aware that Indian society has usually been a cash-driven society and though today, we see a fruit-seller using PhonePe or Paytm for his business, still a large section of Indians is unaware of the knowhow of digital transaction. Thanks to demonetization; that people who used to keep money stored at their homes, now they have started keeping their money in the banks which has resulted in inclusive growth and a greater participation of the citizens in the development of Indian economy. Moreover, the availability of various online payment applications and wallets has simplified the basic financial transactions for the ordinary users.

It was in late 1980s that the need of computerization was felt in the banking industry to make an improvement in customer service and book-keeping. The Reserve Bank of India constituted a committee on computerization in 1988, headed by Dr. C. Rangarajan.

Forbes India, in its report of *'Digital revolution in the Indian banking sector'*[1], recaps the history of the evolution of digitization of Indian banks. It states that banks began using Information Technology initially with the introduction of standalone PCs and migrated to Local Area Network (LAN) connectivity. With further advancement, banks adopted the Core Banking platform. Thus, branch banking changed to bank banking. Core Banking Solutions (CBS) enabled banks to increase

the comfort feature to the customers as a promising step towards enhancing customer convenience through ‘Anywhere and Anytime Banking’. Various Core Banking platforms such as Finacle (developed by Infosys), BaNCS (designed by TCS), FLEXCUBE (from I-flex), gained acceptability and popularity. It was with the opening of the economy in 1991-92 that the process of computerization in the industry got accelerated. A major driver for this change was propelled by rising competition from private and foreign banks. Several commercial banks started moving towards digital customer services to remain competitive and relevant in the race.

The Reserve Bank of India played a very significant role in bringing such revolutionary changes to the banking system. Under its supervision, the private and commercial banks have switched to new technology by way of Bank Mechanization and Automation with the introduction various facilities such as MICR, Electronic Funds Transfer etc. MICR-based cheque processing helped banks use the technique to verify the validity and enhanced the security of signed cheques. Similarly, electronic fund transfer helped customers in transferring money from one account to another without physically visiting the branch. Moreover, the inter-connectivity among bank branches by using common software has resulted in faster and more reliable decision-making process and easy access to data. With the implementation of ATMs, doing transactions has become smooth across the country. And to add more luxury, now we have Cash Depositing Machine (CDM) where we can deposit our money round the clock in the same ATM booth and thus, we can now deposit and withdraw money at the same place.

Expanding Business-From Commercial to Payment banks:

Along with the introduction of Payment Banks, Small Finance Banks and various others app-based platforms of Non-Banking Finance Corporations (such as Navi, KreditBee etc.), a sharp rise in the customer base can be witnessed. Along with this, there is also a rapid surge in applying for Credit Cards as well. With no or minimum documentation, instant approval and by advertising themselves on almost every social media platform, these credit card agencies are successful in luring people to engage in online activities more and more. A large number of their customer base comprises of young people who range between 16-30 years and who are aware of the knowhow of internet-based activities and are also informed about basic digital banking but not much educated about secure banking and financial literacy. As the numbers of unemployed people rose during and after the pandemic, we can see the launch of various mobile apps that offer quick and hassle-free loans to its customers. Despite offering lower amount with high interest rate, these loan and credit card companies (which includes several major banks as well) managed to penetrate money into the

market and kept the wheel of economy moving on. In so doing, these financial entities collects the personal data of their customers and any other user who even just scrolls down their applications or webpages. These data contains simple but private information like Name, Mobile Number, e-Mail Address etc. and these credentials are usually verified by sending One Time Password (OTP) to them. After that, you may choose to leave the app or the web page or may remain there, but your data is now in the market.

Data Protection and Digital Transaction-

The Perilous Narrative:

Rephrasing the quote of Uncle Ben, one may say that 'with greater digital transactions comes greater threat'. And such is the case. Though demonetization pushed people to adopt digital platform for their financial transactions, but it was the Covid era which saw an exponential increase in online transactions, and with this, as it was bound to happen, we witnessed a surge in the rise of digital payment frauds. Seeing a large number of people going digital, fraudsters have started using innovative and novel ways to trap vulnerable customers which lead to disclose their sensitive and confidential information which results in the loss of their hard-earned money. As more people are using contactless payment method, cybercrimes like Phishing, OTP frauds, Ransomware, Malware and Fake UPI links are on the rise. I mentioned about various loan providing apps in previous pages. The interesting thing which we all may notice is that while installing these apps in our mobile phones, they ask us to allow them access to our phone contacts, medial gallery, messages and if we don't do it, then the app doesn't function. I am reluctant to say that these apps are safe and we have nothing to be afraid of, because I am still unable to understand that other companies on whose apps I didn't sign in nor did I apply for a loan, how can they be aware of my requirement and keep sending me various offers to avail their products? It is quite obvious that my credentials are not secured and they are shared with others without my consent and made me a soft and identifiable target of cyber terror. It gives me reason to believe that there is little (or no) room for privacy once our data is taken; no matter whatsoever agency or company or bank it is.

Before advancing further, we need to understand the threats which persist while banking online. Here are a few of them.

1. **Phishing:** In her book, "Cyber Crime", Dr. Talat Fatima defines the term "phishing" as a variant of fishing, probably influenced by *phreaking*.[2] This trick urges the victim to enter into a link thereby arresting him within the apparently innocuous looking Net but actually inviting him to a malicious attachment or link. Often a phone is received by the user

apparently originating from a bank asking the victim to dial a phone number authorized to solve their banking problems. Once the number is dialed the user enters the account number or PIN. Thus, phishing is an attempt to acquire the sensitive information of the victim.

She also speaks of ***Vishing*** which is also known as phone phishing in which the phoning device is used to enter the personal information of the customers.[3] It is the exploitation of the user's trust in telephone services where the caller ID spoofing and complex automated systems are used to commit vishing. The technique used in it is the fraudsters takes advantage of the weakness of a public booth (Public Branch Exchange or PBX) connecting to the voice over Internet Protocol (VoIP) services and "auto-dial" thousands of people in just a few hours. They employ the following techniques:

a. List of phone numbers are stolen from a financial institution and a "war dialer" is used to make calls in a limited region.

b. Such caller then warns the consumer that some malicious activity is detected on their credit card or bank account; hence they should make a call to the bank instantly.

c. The moment the anxious consumer makes such instructed call, the automated but unauthorized number asks the consumer to enter their credit card number and other credentials.

Such intimated credentials serve the purpose of the fraudster who ultimately misuses it.

2. **Data Extraction:** An insecure internet connection always brings opportunities for cyber criminals to enter your network and steal your data therefrom which includes our username and password which we use for net banking and other digital transactions. If internet is like a stream, then these cyber attackers could be termed as alligators that keep searching their prey.

3. **Mobile Malware:** Mobile malware is malicious software which is designed to target the operating systems of smartphones. It collapses the operating system and leaks our private data stored in the phone. By using mobile malware, the fraudsters not only can access our banking details through the banking apps in our phone, but also can extract other data that are stored in our device. Needless to say, all these will simply result in loss of money from our bank accounts.

4. **Duplicating SIM Cards:** Cybercrime has both virtual and physical aspect. One such physical aspect is duplicating SIM card which requires stealing of a mobile device. It is easy to duplicate our SIM card of our stolen mobile. If it happens, then we will not receive calls

and messages anymore, but all the data of our SIM card is copied to the duplicate SIM. The duplicate SIM captures the exact behavior of our original SIM, which means that the attacker can conduct transactions involving the use of data stored on your SIM cards.

The list of threats to digital banking could be a bit longer but the above mentioned particulars are widely used by the cyber-poachers and one needs to learn and aware about them.

Enforcing the Law-The Road Taken:

The Indian Banking system is duly regulated with an array of laws which includes The Reserve Bank of India Act, 1934; the Banking Regulations Act, 1949; the Foreign Exchange Management Act, 1872; and the Bankers Book of Evidence Act, 1891. Moreover, the Indian Evidence Act, the Negotiable Instruments Act and the Indian Contract Act have also their role in our banking system. To be precise, all these laws are also applicable to the Internet Banking in India and the remaining requirement of Internet Banking is fulfilled to some extent with the passing of the IT Act (amended in 2008). The IT Act, 2000 (as amended 2008) has encircled within its ambit several new infractions as cyber-crime. Some sections which are relevant in the context of Internet Banking are being mentioned here: [4]

a. Section 43-A: If a Body Corporate while handling personal data, does neglect to protect then it shall be liable to pay damages by way of compensation to such person. The handling of such personal data should be strictly in accordance with the security practices and procedures as laid down now in Rule 8 of the IT Rules, 2011.

b. Section 66-C speaks about Identity theft. Whoever fraudulently or dishonestly makes use of electronic signature, password, or any other unique identification figure of another person, he shall be punished with an imprisonment up to three years and a fine of Rs. 1 lakh.

c. Section 67-C states that intermediaries should preserve and retain information in prescribed manner and its violation is a punishable offence which can be up to three years imprisonment and fine.

d. Section 70 is about disclosure of information by an authority having access to it without the consent of the person concerned. Punishment includes imprisonment up to two years or fine up to Rs. 1 lakh or with both.

e. Section 72-A concerns about a body corporate which has access to the personal information of a person under a contract and if such body discloses it to another with the intention of

causing wrongful loss or wrongful gain to anyone, then it will be punished with imprisonment up to three years or with fine up to Rs. 5 lakh or with both.

'actus non facit reum nisi mens sit rea' (no act is an offence unless done with a guilty mind), is the cardinal principal of criminal law. The Indian Penal Code, the time tested and most widely used substantive criminal law in India, has many offences contained therein which can be swiftly applied for offences regarding Internet Banking. Given below are the sections of IPC that can be applied.

1. Theft. (Ss. 378 & 379)
2. Extortion. (Ss. 383 & 384)
3. Criminal Misappropriation of property. (S. 403)
4. Criminal breach of trust. (Ss. 405 & 406)
5. The offences of "forgery" and "making of false document" have been defined in Section 463 and section 464(c), in relevance to the electronic record and affixing electronic signature as well.
6. Sections 415 & 420 contain the offences of fraudulently or dishonestly inducing a person to deliver property etc. Since these offences too, can be done by using electronic devices, hence they have been taken under the purview of the IPC along with the relevant sections of the IT Act.

Apart from this, we have the provision of 'Internet banking and the Payment and Settlement Systems Act, 2007' which authorizes the RBI to act in respect of offences punishable under this Act. Under it operating a payment system without authorization, failure to comply with the terms of authorization, failure to produce statements returning information or documents, providing false statements of information, disclosing prohibited information and non-compliance of directions of RBI are all labelled as offences.[5]

It brings us hope and solace when we see that our government is committed and serious about curbing the menace of terror, be it physical or digital. Apart from establishing cyber-crime department under the Ministry of Electronics and Information Technology (MEitY), the government has come with *'Digital Personal Data Protection Bill, 2022'* which has provisions to regulate the method and means of obtaining and use of our personal data and I believe that it will minimize the existing call of threats once it is passed and comes into force. It is very interesting to find that twenty-one years back, the Reserve Bank of India had set up a 'Working Group on Internet Banking' to examine different aspects of Internet Banking which focused on three major areas, i.e. technology

and security issues, legal issues and regulatory and supervisory issue. The RBI, in its six paged Internet Banking Guidelines (vide memo no. DBOD.COMP.BC.No.130/07.3.23/2000-01, Dated: 14th June 2001)[6], had clearly instructed all scheduled commercial banks regarding Internet Banking and the issues related with it, some of them were:

a. Banks should have a security policy duly approved by the Board of Directors.

b. Banks should introduce logical access control (such as User ID, Passwords, smart cards or other biometric technologies) to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc.

c. Banks should use the proxy server type of firewall so that there is no direct connection between the internet and the bank's system.

Moreover, the RBI kept issuing various orders and guidelines from time to time in order to regulate internet banking and digital transactions. The commercial banks, on their part, have also worked to comply with the instructions of the RBI so far.

Apart from this, considering the growing risks and threats from Cyber warfare, in its guidelines for Cyber Security Framework (2016)[7], the RBI made a clear distinction between cyber security and information security. Information Security is related with protecting confidentiality, integrity, and availability of information whereas Cyber Security is all about protecting or defending the use of cyberspace from cyber-attacks. It is just an interconnected network of information system such as internet, telecommunication networks, computer systems, embedded processor and controllers and many other systems. Since traditional information security has its limitation in covering of risks emanating from cyber space such as Cyber warfare, negative social impacts of interaction of people, software and services on the internet and threats from Internet of Things (IoT), hence all these aspects are included in Cyber Security. These are not classic information security issues and thus covering them under a separate Cyber Security Framework is needed.

The Conclusion-A Long Walk to Secure Banking:

Even though the number of financial fraud and cyber-attack is on the rise, we must understand that every act of development brings challenges of its own kind. The main reason behind such rise is the lack of ***'figital literacy'*** (financial and digital literacy) among a large section of our society. Even our young generation is not digitally and financially literate enough to understand these hidden traps. Mere using of internet banking with strong password is not sufficient. Gone are the days when fraudsters use to ask our Debit/Credit Card number, CVV Pin, OTP etc. They have found (and will

keep exploring) new ideas and medium to dupe us and will do their best to cause serious harm to us. In such scenario, we also need to change our strategy and should make necessary arrangements so that we may avoid such tricks and threats. Steps like having a strong net banking password (and to change it frequently), secure internet connection, avoid using public Wi-Fi network, using authentic anti-virus in mobile/computer, not responding to unknown and strange calls/SMS or open any insecure or suspicious web link are some useful methods which will enable us in avoiding such malicious threats. But even after using all precaution if we still suffer any loss or damage then we don't need to remain mute spectator but to file a complaint on the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) and let the law take its own course. Apart from this, the aggrieved person may also lodge complain about the cyber-crime at the designated cyber-crime police station of the concerned district. Moreover, the district or police administration along with the civil society group or NGOs, also needs to create awareness in the public by:

a) Driving campaign on regular basis,

b) Putting hoardings/posters, mentioning about the knowhow of financial fraud,

c) Encourage public to complain about cyber-crime,

d) Drive campaign on social media platforms and make the public understand the nitty-gritty of cyber-crime by simplifying them in reginal languages, etc.

The list is not exhaustive, but we need to understand that things are changed with the changing times. We don't become smart just by using an expensive mobile phone. There is much to learn about it. Since we cannot think of our future without internet banking or digital wallets and other apps like that, therefore it is highly imperative for us to learn and understand the usage of these digital tools. The wheel of law will never move until we drive it. Hence, we must report all such incident of financial fraud to the concerned authority, and I do believe that our legal system is strong and capable enough to curb and crush this menace slowly but very, very effectively.

****

Bibliography

1. https://www.forbesindia.com/article/weschool/digital-revolution-in-the-indian-banking-sector/47811/1

2. Talat Fatima, Cyber Crimes 436, (Eastern Book Company 2021)

3. Talat Fatima, Cyber Crimes 438, (Eastern Book Company 2021)

4. IT Act, 2008, No. 10, Acts of Parliament, 2009 (India)

5. The Payment and Settlement Systems Act, No. 51, Acts of Parliament, 2007 (India)
6. https://m.rbi.org.in//scripts/NotificationUser.aspx?Id=414&Mode=0
7. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-rbi-guidelines-for-cyber-security-framework-noexp.pdf

################