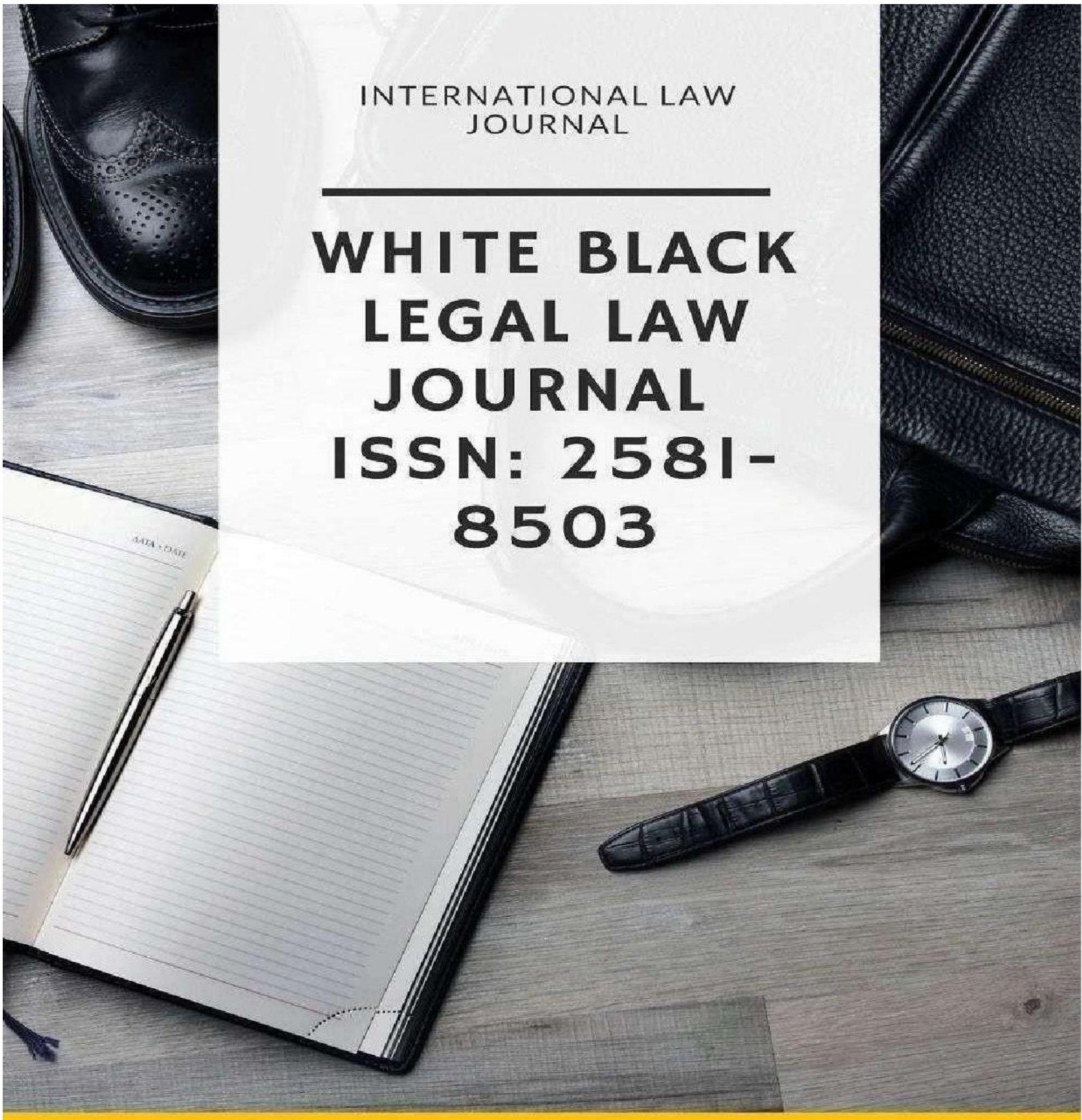


INTERNATIONAL LAW JOURNAL

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.

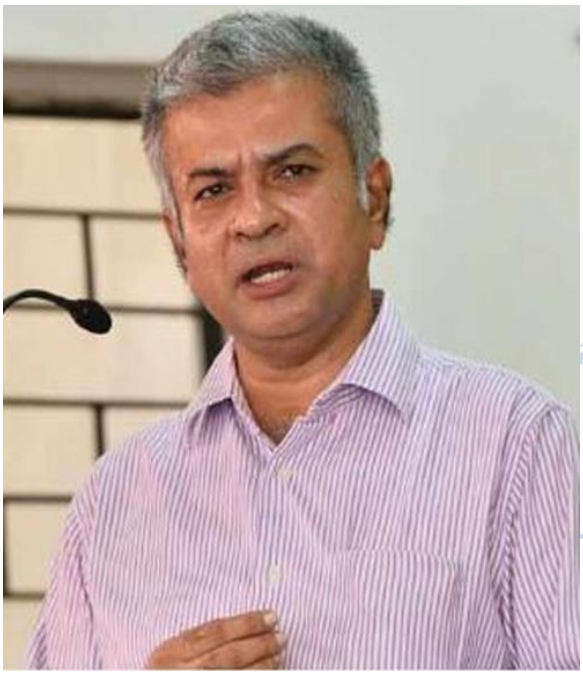
WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Editor In Chief

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 professional 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

The Net Misdemeanor On Banknotes

Authored By-Milan Donson

Abstract

The Internet is a global -network that connects with the computer and in exchange of information. The Internet made information for everyone .The Life and moving of life became easier and moving of life with more technological. From the easier and technological way, some people take more advantage ,as getting into an unauthorized access. The getting into an unauthorized access through without consent can be termed into 'cyber crime'. Cyber Crime is biggest and latest complicated issues facing by the advanced world. Cyber crime can be done against individual or individual property ,against an organisation, against society .The Cyber crime can be in the form of fraud ,data theft etc. The main and frequent way on

Cyber crime is in banking .Because banking is not only done with knowing people ,transaction can be made to an third party also. Here the unauthorized way of interfering into the transaction between them is most terrible and unknowingly .The transfer of fund, getting into the down payments made ,knowing the passwords and files these all will into cyber crime. The Cyber crime not only became challenge to the growing technologies ,it is a great challenge to the infringement of an individual privacy .In India, traditional way of banking like banking on basic paper based instruments like cheques ,pay-in-slips is on the way to the electronic banking i e, 'e-banking'. The way of doing crime in traditional way to cyber way is much new-fangled ,even the person involved in cyber crime will be in the behind the screen only .The much of money is increasing day by day as due to the economic factor ,here the people will involve in more ways to carry money like e-wallets and other operations. The Crime will not restrict to banking only, even it is a way to the 'Cyber Terrorism'.

Keywords: Cyber Crime, E-Banking, Cyber Terrorism

Introduction

From the difficulty to detect and even more difficulty to prove ,the cyber crime has many unconventional way of committing crime .As keeping it away ,as the new advanced level of banking helps in speedy payments and settlement stratagem. As the part of progress the traditional using of ATM cards has changed to online banking and to internet-related crimes. Before to the sudden expansion of banking sector ,the crime was mainly targeted on the outside boundaries of internet ,but when users and thinkers became mechanized ,the pattern of crime became much closer to the victim .The Cyber frauds has mainly discernible in the area of cash involvements .The pattern of committing crime with unseen face an motive. [1]Digital banking makes it easy and convenient for consumers to manage their financial lives, including doing everything from paying bills to sending money to shopping online. And that's become especially important as the Covid-19 pandemic changes the way people carry out banking tasks. In the latest World Retail Banking Report, 57percentage of consumers say they now prefer internet (online) banking to traditional branch banking. And 55percentage of consumers now prefer using mobile banking apps to stay on top of their finances, up from 47percentage in the pre-pandemic era. According to a 2020 study published by KPMG, 87percentage of consumers say data privacy is a basic human right. Yet 68percentage say they don't trust companies to ethically sell their personal data .In the case of [2] *Mphasis BPO Fraud (2005):* In December 2004, four employees of Mphasis, working at an outsourcing facility in India, obtained PINs from four customers of the company's clients based in the U.S. They were not authorized to do so; but they impersonated that to have the authority and with details obtained, they opened new bank accounts using false identities. Within a couple of months, they used the credentials and transferred all the money from the bank accounts of the clients (in the U.S.) to their new accounts at Indian banks. By April 2005, the Indian police had been informed by the U.S. bank of the scam, and post-investigation, the individuals involved in the scam were arrested. It was informed that an amount of $426,000 was stolen, out of which $230,000 was recovered.

[1] https://www.forbes.com/advisor/banking/digital-banking-consumer-data-privacy-concerns/

[2] https://blog.ipleaders.in/cyber-law-vis-vis-net-banking-indian-sector/

The arrests were made successfully when these fraudsters tried withdrawing the cash from the Indian bank account. The Court held that the nature of the crime was that of unauthorized access to commit fraudulent transactions. [3]

Check Point's "Mobile Security Report 2021" lists a 15% increase in global banking Trojan activity in 2020, threats that put mobile users' banking credentials at risk as threat actors have been using mobile remote access Trojans (MRATs), banking Trojans, and premium diallers often hidden within apps claiming to offer COVID-19-related information in 2021, thus making mobile banking apps fertile ground for cyber attacks and one of the biggest risks for the banking industry.

[4] In India in the case of *Umashankar Sivasubramaniian v. ICICI Bank* (Civil Petition No. 2462/2008, Adjudicating Officer of Judicature of Chennai) – The complainant, Mr. Umashankar, alleged that his bank account was wrongfully debited on account of negligence on the part of the bank. The Bank contended that the case refers to phishing and blamed negligence on part of the complainant and was of the opinion that the matter cannot be brought under the purview of the IT Act and that the complainant must lodge an FIR. The Adjudicating Authority vide its order held that the ICICI bank had failed to establish that due diligence was exercised to prevent the breach, found that the Bank was guilty of the offenses made out in Section 85 read with relevant clauses of Section 43 of the IT Act and directed ICICI Bank to pay to the complainant a total sum of Rs. 12,85,000/- (Rupees Twelve Lakh

Eighty-Five Thousand only). The bank had obtained a stay and an appeal was filed before the Cyber Appellate Authority.

By Hacking or by an e-mail attacks, it can break a threat to the sovereignty of a country .In

India ,all the legal transactions, electronic data exchange are guided by the IT Act 2000.The Reserve Bank of India (RBI) has given guidelines to the banks for the protection and secureness of e-banking like the facilities of three-step -authentications. To some extent it keeps the doing the e-banking transparent and secure .But there is evils happening beyond the laws and regulations .This paper says the Cyber crimes and law which affects the banking sector and which is going to affect the banking sector by the technological and economical effect due to the advancement of the world.

[3] https://www.crn.in/columns/securing-modern-e-banking-services-for-banks/

[4] https://blog.ipleaders.in/cyber-law-vis-vis-net-banking-indian-sector/

Literature Review

Pauledison and Ramesh (2018) states that ubiquitous and prevalent online threats about hackers, identity theft, stolen password, viruses, warms and spyware tend to make customers wary just like in any other country. These customers are also not sure about the efficiency of banks websites and their commitment to allocate funds for reliable encryption mechanisms and robest back-end technologies and systems.

Anuja and Thakur (2017) states the biggest pitfall of the internet banking scheme which needs to be guarded against by the common customer hacker attacks, phishing, malware and other unauthorized activity are not uncommon on the net. Most banks have made it mandatory to display scanned copies of cleared checks online to prevent identity theft. It is essential to checks online to prevent identity theft. It is essential to check bank's security policies and protections while opening an account and commencing the usage of online backing facilities.

Monisha , et.al, (2017) states that risk of revelation of not to be disclosed or confidential information & alarm of identity theft is one of the major reasons that restrain the consumers while opting for electronic banking services. Traditional banking is often used by customers because of lack of conviction in the online bank transaction. The bank may march into their confidentiality by using their information for marketing and other purposes without agreement of consumers.

Nidhi (2016) mentioned that trust is among the significant factors which influence the customers willingness to engage in transaction with web merchants. A large group of customers refuses to opt for e-banking facilities due to uncertainty and security concerns. Around 50% of internet users are not using internet banking in India because of security concerns.

Kumar (2017) states that transferring a large amount of money, security is a significant factor of online banking. It is taken very seriously during online banking procedures. Most of the people seen to believe that it is a hacker jungle out there and stay very wary so simplifying their lives by using cyber space even though it has became a standard and convenient way of banking.

Ramesh and Muthumani (2017) identify that the confidentiality, integrity, authentication, this three are very important features of the banking sector and where very successfully managed all over the

world before the coming of internet. Communication across open and insecure channels such as the internet might not be best base for bank-client relations as trust might partially be lost.

Sriram and Sai(2018) mentioned that conservative Indian Bank customers used to years of saving in an erstwhile mixed-socialist economy are always fearful of losing hard-earned savings in online scams .These customers are also not sure about the efficiency of banks.
Since they value their customers ,they always use the most advanced security technology in protecting their website.

Senthilkumar (2018) identify that the risk of disclosing private information and fear of identity theft is one of the major factors that inhabit the consumers while opting for internet banking services .Most of the consumers believe that using online banking services make them vulnerable to identity theft. According to the study consumers warry about their privacy for information shared and saved for the financial transaction purpose.

Anitha (2019) mentioned that right now with low and lack of adequate security ,infrastructure and internet penetration, it is significant to take necessary actions to enchant e-banking. Information technology provides security and legal framework for e-commerce transactions as well e-banking. Information Technology Act or RBI suggested that criterion of Digital Signature Certification Board for authentication of electronic records and communication with digital signatures.

Gupta, et.al (2021)noted that basic challenge for banks to persuade the users on this element ,which may in advance establish the internet banking operation. The users have some confusion or question about whether the dealing is completed before receiving the confirmation message.

Research Question

i) How Cyber Crime on banking can be controlled?

Objectives

The main objective of this paper is to identify the Cyber Crime on banking and measures to control the cyber-crimes by cyber laws.

Methodology

Present Study is mainly based on secondary data collected from various sources about available information on the breakthrough of transgression on money matters. Also the secondary data has been collected from different sources which include the official data as well as available literature on the subject from different journals, books, articles , newspaper etc.

Study Results

The private information is exposed and concerns about frauds are the main elements which made the customers to bring backward in using e-banking .The bank assures a safe banking by steps for resolving the security and other concerns by :

-)Keeping security concerns in mind ,all banks in India must follow a standard. Also, the banks Association should design this standard.

-)All banks must adopt adequate security measures to maintain the secrecy and confidentiality of data .Further ,they must use logical access control to implement it.

-)In Order to mitigate the money laundering risk , banks must develop an Anti money laundering (ALM) technology for reporting and querying.

-)Banks must have an internal grievance redressal system to adopt a fraud-free culture of banking.

-)All banks must have an explicit security plan along with documentation .Further ,banks must strictly ensure physical access control.

Privacy on the different hand become another threat in doing the e-banking .The effect of privacy will affect the customers knowingly or by unknowingly .In India ,The National Crime Records Bureau (NCRB)however presents a different set of data. According to NCRB

,India reported 50,035 cyber crime in 2020.44,546 cases in 2019 and 27,248 cases in 2018 .The year 2020; 4,047 cases of online banking fraud ;2160 cases of ATM fraud;1194 credit/debit women and 578 cases of fake news on social media ,NCRB data showed.

Source: https://www.news18.com/news/india/cyber-crimes-in-india-spiked-nearly-ninetimes-since-2013-up-topped-chart-in-2020-data-4210703.html

Case Laws

i)In the case of *Manoj Kumar Rai vs The State Of Jharkhand* on 4 March, 2021

It has also been stated in the letter on the basis of certain newspaper reports that 5024 cases have been registered in the last year of 2020 in Jharkhand State alone and the customers are in danger of suffering fraud in absence of proper safety system mechanism in the banks. It has also been complained that the system operating are opaque and do not respond the issues raised by the affected customers. The fraudsters usually start with phishing and sharing personal data and then carry on navigating freely, unchecked by the system which may not be possible if proper alerts and checks are inbuilt in the system. It has also been brought in notice by the letter that single OTP sharing by the customers is the sole explanation by the banks for putting blame on the customers who have been subjected to the fraud. The system does not stop fraudulent transactions in spite of unfamiliar pattern of transactions, frantic in nature, etc. It is stated in the letter that the Banks usually avoid such questions and take cover of system which itself requires updating to meet the menace with a strict safety norms. It has further been informed that the banks profiting by promoting the internet and digital banking require to be more responsive to help the fraud victims instead of refusing their claims. The real threat of misuse of such money siphoned by the fraudsters due to laches in the system by some antinational activities may also be possible and it is a serious

concern for the administration also.[5]

ii) In the case of, *Pps International vs Punjab National Bank* on 14 June, 2022

The opposite party filed its written reply on 11.11.2009 in which, the material facts have not been denied. It has been stated that the complainant opened Current Account vide Account No.2726002100046578, in PNB Branch at Sector-27, Noida, w.e.f 05.05.2006 with Smart Roamer Account facility. PNB started Internet Banking Services in August, 2003 with the approval of Reserve Bank of India as per RBI guidelines issued in June, 2001. Internet banking facility is available to retail customers and corporate customers on all the branches of PNB. For corporate Internet Banking, the corporate has to submit resolution of the Board of

Directors, authorising a particular person for using the services. Internet Banking system of PNB was fully secured and in conformity of international standards. The PNB has employed all security measures which were internally acclaimed and reputed. For operating Internet Banking, login identity and password was issued to the complainant. Without login identity and password, account cannot be operated through Internet Banking. The website of PNB can be accessed from links www.netpnb.com and www.pnbindia.com. First page of the website displays the following important notice/icons to all the visitors/account holders i.e. important message, security features, safeguards, Precaution for net banking and Beware of fraudulent mails. On clicking on aforesaid links, respective window will open, wherein detailed guidelines have been given by the bank regarding use of internet facility and how to secure against any email frauds. The bank emphasizes that the bank will never contact any of the customers and ask for login details or password or any other personal information over email. The bank provides that the customer should be beware of fraudulent website deceptively similar to PNB's banking website of scam emails which may contain virus or be linked to fraudulent website. The bank always insists to look at the padlock symbol on the right hand corner of the web page to ensure that the customer is connected to secure PNB's website and the customer should logout, when he/she intends to exit internet banking to ensure that the secured session is terminated. The opposite party has provided a checklist while accessing the account through internet as under , Keep user ID and password a secret, select password which is difficult to guess, Never write or disclose your password to anyone including officials in the bank, Destroy the password mailer after changing the password, change the

[5] https://indiankanoon.org/docfragment/199569901/?big=0&formInput=internet+ban king+fraud

password periodically, Use all virtual/dynamic keyboard shown on the screen to enter the password Avoid accessing internet from cyber café or share network, Protect the computer with adequate anti-virus solution and Never click on a website link/attachment in unknown/suspicious email. Due to fault of the complainant, important data of login identity and password might have leaked, on the basis of which unauthorised transaction were made. The complainant has lodged FIR of the incident. The police is investing the case and may come to a definite conclusion. Although Rs.54/- lacs has been recovered during investigation but involvement of the employees of PNB in the incidents has not been surfaced.[6]

IT Act And Amendments

Privacy and Security are the main part of doing banking transactions for the companies to the individuals .The IT Act provides a legal guard for the consumers information accessed by the unauthorized access by various features likes digital signatures, the appointment of controller of Certifying Authorities, safeguards to banking sector like steps authentication facilities for banking. From the part of the government majority of cyber crime in India are bailable offence these became most distinguishable issue in this protection stage of cyber-crimes. In the IT (Amendment) Act, 2008 made all most all cyber-crimes on bailable offences.

[7]This amendment introduced the controversial Section 66A into the Act.

Section 66A

Section 66A gave authorities the power to arrest anyone accused of posting content on social media that could be deemed 'offensive'. This amendment was passed in the Parliament without any debate. As per the said section, a person could be convicted if proved on the charges of sending any 'information that is grossly offensive or has menacing character'. It also made it an offence to send any information that the sender knows to be false, but for the purpose of annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, through a computer or electronic device. The penalty prescribed for the above was up to three years' imprisonment with fine.

[6] https://indiankanoon.org/docfragment/66418736/?big=0&formInput=internet+banking+fraud

[7] https://byjus.com/free-ias-prep/information-technology-act-

Arguments Against Section 66A

Experts stated that the terms 'offensive', 'menacing', 'annoyance', etc. were vague and illdefined or not defined at all. Anything could be construed as offensive by anybody. There was a lot of scope for abuse of power using this provision to intimidate people working in the media. This also curbed the freedom of speech and expression enshrined as a fundamental right in the Constitution. The section was used most notably to arrest persons who made any uncharitable remarks or criticisms against politicians. The government contended that the section did not violate any fundamental right and that only certain words were restricted. It stated that as the number of internet users mushroomed in the country, there was a need to regulate the content on the internet just like print and electronic media. The Supreme Court, however, in 2015, struck down this section of the IT Act saying it was unconstitutional as it violated Article 19(1)(a) of the Constitution. This was in the famous *Shreya Singhal v Union of India* case (2015).

Section 69A

Section 69A empowers the authorities to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defense of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.It also empowers the government to block internet sites in the interests of the nation. The law also contained the procedural safeguards for blocking any site.When parties opposed to the section stated that this section violated the right to privacy, the Supreme Court contended that national security is above individual privacy. The apex court upheld the constitutional validity of the section. Also read about privacy laws and India. The recent banning of certain Chinese Apps was done citing provisions under Section 69A of the IT Act. The Indian Telegraph Act, 1885 allows the government to tap phones. However, a 1996 SC judgement allows tapping of phones only during a 'public emergency'. Section 69A does not impose any public emergency restriction for the government.

Information Technology Intermediary Guidelines (Amendment) Rules, 2018

The Rules have been framed under Section 79 of the Information Technology Act. This section covers intermediary liability. Section 79(2)(c) of the Act states that intermediaries must observe due diligence while discharging their duties, and also observe such other guidelines as prescribed by the Central Government.

Online Intermediaries:

An intermediary is a service that facilitates people to use the Internet, such as Internet Services Providers (ISPs), search engines and social media platforms.

There are two categories of intermediaries:

Conduits: Technical providers of internet access or transmission services.

Hosts: Providers of content services (online platforms, storage services).

Information Technology Intermediary Guidelines (Amendment) Rules were first released in 2011 and in 2018, the government made certain changes to those rules.In 2018, there was a rise in the number of mob lynchings spurred by fake news & rumours and messages circulated on social media platforms like Whatsapp.To curb this, the government proposed stringent changes to Section 79 of the IT Act.

According to the 2018 Rules, social media intermediaries should publish rules and privacy policy to curb users from engaging in online material which is paedophilic, pornographic, hateful, racially and ethnically objectionable, invasive of privacy, etc. The 2018 Rules further provide that whenever an order is issued by the government agencies seeking information or assistance concerning cybersecurity, then the intermediaries must provide them the same within 72 hours. The Rules make it obligatory for online intermediaries to appoint a 'Nodal person of Contact' for 24X7 coordination with law enforcement agencies and officers to ensure compliance. The intermediaries are also required to deploy such technologies based on automated tools and appropriate mechanisms for the purpose of identifying or removing or disabling access to unlawful information. The changes will also require online platforms to break end-to-end encryption in order to ascertain the origin of messages.

Now presently Government Initiatives for Cyber Security are :

-)Surakshit Bhart Initiative

-)Cyber Swachta Kendra

-)Online Cyber Crime reporting portal

-)Indian Cyber Crime Coordination Centre
-)National Critical Information Infrastructure Protection Centre (NCIIPC)

The Government is looking at a new legislative framework with the new rulemaking capabilities that deals with various issues related to digital space with the majority of cybercrimes need to be made non-bailable offences .A comprehensive data protection regime needs to be incorporated in the law to make it more effective.

Findings

This research paper shows that ,there should be some measures from the side of bank to control the cyber crime on e-banking:
-)Encrypted email messaging

-)Three -step authentication

-)Electronic signature verification

-)Continuous account monitoring

-)Automatic logout function

-)Backup & Recovery

-)Deactivation of login after several incorrect attempts

-)Privacy protection training for customers

Even there is protection from the bank for doing the safe banking ,there is need of protection from users itself:

-)Choose trustworthy financial apps

-)Be wary of phishing scams

-)Sign up for banking alerts

-)Steer clear of public Wi-Fi

-)Choose strong and unique password

Conclusion

E-banking provides facility of transfer of money through any parts of the world at any time .The e-banking not only helps in the advancement for the bank, it will also make the advancement in the customer involving in the online banking. The drive towards e-banking makes banking more easier for the customers, but the same time the bank should provide the most convenient way of e-banking by giving most updated application for increase the effectiveness and efficiency and create awareness on usage of e-banking for secure use of ebanking. The safety and security are the main challenge in providing good e-banking services. There should be awareness from the bank and customers should also be aware of problems in using of online banking and what made them from not using of online banking services .Even though the legal framework provide a guard on online banking .The users itself should known what they are doing. The main part of cyber crime is that there is no face to face interaction with the accused and with the victim. The vigilant use of e-banking itself is needed from the customers itself .The sharing of credentials and data's to a unauthorized access, these all can lead to cyber-crime. The security stability of e-banking also connected with the security of the gadget using for the purpose of banking. The passwords ,security pin number ,data's authentication pin all these instruments needs a extreme of security .Any unauthenticated access of passwords and pins will affects to the security and privacy .This fraud even leads to the gain access of bank credentials.

References

- Anitha.K,A (2019), Study on Challenges and Opportunities in E-Banking Sector in India , New Frontiers in Business, Management and Technology, Vol.7.
- Anuja Bhadauria and Thakur K.S , (2017), A Conceptual Study of challenges for ebanking scheme with refence to Commercial Bank in India, Journal of Advances and Scholarly Researches in Allied Education ,Vol.12,Issue No.2,January 2017
- Kumar Akshaya Bhandary (2018), Prospects and Challenges in E-Banking :A perception study.
- Sriram Devulapalli, Karthik Sai Orugati (2018) ,Challenges and Opportunities of ebanking in India,IOSR-JBM,PP 56-61
- Ruchi Gupta, Amit Mittal, Bhagabat Barik, (2021), A conceptual study on emerging challenges towards e-banking ,*Research Journal of Management Science* ,Vol 10(3),PP 34-39,September 2021
- Pauledison Lawrence, Ramesh R P, (2018), A Study on challenges of internet banking with reference to Chennai city, IJCMR ,Vol.4,Issue 4,July 2018
- Monisha , Kanika Bhudhiraja, Jatinder Kaur (2017), Electronic Banking in India :Innovations Challenges and Opportunities ,IJERT ,2017
- Kumar Nidhi (2016), E-Banking in India :Challenges and Opportunities ,IJSTM ,Vol.No.5,Issue 8,August 2016
- Ramesh.L, Muthumani.A (2017), Electronic Banking in India ;Challenges and Opportunities ,IJSTM ,Vol.No.6,Issue No.2,February 2017
- Senthilkumar.C, (2018), E-Banking in India: Challenges ,JETIR,Vol.5,Issue 12,December 2018
- https://www.forbes.com/advisor/banking/digital-banking-consumer-data-privacyconcerns/
- https://blog.ipleaders.in/cyber-law-vis-vis-net-banking-indian-sector/
- https://byjus.com/free-ias-prep/information-technology-act2000/#:~:text=The%20Information%20Technology%20Act%2C%202000%20was%20enacted%20by%20the%20Indian,and%20also%20to%20prevent%20cybercrime

- https://www.crn.in/columns/securing-modern-e-banking-services-for-banks/
- https://indiankanoon.org/docfragment/66418736/?big=0&formInput=internet+banking+fraud
- https://indiankanoon.org/docfragment/199569901/?big=0&formInput=internet+banking+fraud
- https://www.news18.com/news/india/cyber-crimes-in-india-spiked-nearly-ninetimes-since-2013-up-topped-chart-in-2020-data-4210703.html
- https://www.toppr.com/guides/business-economics-cs/money-and-banking/risks-ofe-banking/#:~:text=Security%20Risk,-When%20we%20talk&text=All%20customers%20want%20their%20transactions,access%20to%20the%20bank's%20systems
- https://zeenews.india.com/technology/two-months-of-2022-saw-more-cybercrimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb-2458733.html
- https://www.drishtiias.com/daily-updates/daily-news-analysis/need-for-new-it-law