ONLINE FINANCIAL FRAUDS AND CYBER LAWS IN INDIA -AN ANALYSIS

Upasana Ghosh
Assistant Professor of Law, Bikash Bharati Law College, University of Calcutta

ISSN 2277-7733
Vol. 10, Issue 1, June 2021

Abstract

With the advancement of technology, data protection and data privacy have become a major concern. People are mostly occupied by the internet, computer and mobile phones nowadays. From buying medicines, cosmetics, grocery items, food, clothes etc, or finding a groom or bride, or managing finances, people are dependent on online apps or websites, which often lead to breach of private data if not used cautiously. Data protection is now under threat by the interference of strangers. Thus, in this study, an attempt has been made to explore the viewpoint of the netizens on online financial transactions and whether the existing cyber laws in India are giving sufficient protection to the right of privacy and confidentiality of the netizens.

***Keywords**: technology, internet, cyber security, financial frauds, law, netizens*

We all are now acquainted with using mobile phones, tablets, laptops, computers and other electronic gadgets. Since internet is easy to use, there are no geographical barriers, services can be afforded with minimal cost and we can get everything at the tip of our fingers with less effort, we have become more reliant on it. However, most of us are unaware of the insecurity of the internet, the websites or apps which we follow regularly. Due to this, the scammers get an opportunity to mislead innocent people and loot their hard-earned money. Cyber crimes are carried out over the internet, computer, mobile phones, email, etc with intent to steal personal details, incur financial losses, damage to reputation, thereby infringing the right to privacy of netizens. Online financial frauds which include hacking (illegal access to one's computer or computer resource or destroying it), phishing (emails from fraudsters representing them to be reputed companies to gain personal information), email or spoofing (creation of email messages with a forged sender address), carding (stealing someone's credit card details and use for personal benefits), vishing (fraudulent practice of making phone calls or voice messages representing them to be reputed companies to steal personal information) have become very common cyber crimes in the digital world.[1] Internet banking services include mobile banking, phone banking, financial transactions through debit card or credit card, electronic fund transfer. Though India got its first codified legislation on cyber crimes in the year 2000, which is The Information Technology Act, it has failed to become a strong legislation

[1] https://www.stthomas.edu/publicsafety/prevention/fraudidtheft/phishingpharmingvishingsmishing/ as on 03-05-2021

for online financial frauds. In this study, the viewpoint of the netizens on online financial transactions has been surveyed and the current cyber law in India has been analyzed to find out whether the emerging cyber issues on internet banking have been well addressed in the legislations.

Literature Review

Literature review guides the path through which a researcher go ahead with the study. It is an initial part of the research. It helps the researcher to fill up the lacunas left behind by the previous authors. The author has referred to 'Cyber Laws' by Justice Yatindra Singh, 'Cyber laws & Information Technology' by Dr. Jyoti Rattan and Dr. Vijay Rattan' and various books, journals, articles, newspapers for conducting the study.

Objectives of the Study

The emerging crimes on online financial transactions have compelled the author to conduct the study. The objectives of the study are to gather information on the attitudes of the netizens regarding online financial transactions, to understand the type of frauds on digital payments which are arising at a rapid rate and whether the prevailing legislations in India covers the emerging frauds on online transactions.

Research Methodology

Research methodology is the most significant part of research. Partly empirical and partly non-empirical method has been used by the author to conduct the study. For the empirical study, questionnaire has been used as a tool for data collection. Questionnaire was sent to 45 netizens via email, whatsapp, facebook messenger to collect their viewpoint on online financial transactions. The study was limited to the city of Kolkata, West Bengal, India. The data collected has been analyzed and demonstrated in a tabular form by calculating percentage to bring out conclusions. In the non-empirical part, data has been taken from primary and secondary sources. Statutes, legislations, case studies have been referred for primary sources and journals, magazines and websites have been referred for secondary sources.

Historical background of internet banking in India[2]

The historical origin of internet banking in India can be traced back to the 1990s. The credit of launching internet banking in India goes to the ICICI bank. In 1999 Citibank, Induslnd Bank and HDFC followed with internet banking services. The Government of India as well as the Reserve Bank of India took various measures to ease the development of internet banking in India. The Information Technology Act, 2000 was enacted by the Government of India with effect from 17th October, 2000 which provided legal recognition to electronic transactions and provisions to deal with e-commerce. The

[2] Chandrawati NIrala, Dr, BB.Pandey, 'Evolution of e-banking in India- An Empirical Study'

Reserve Bank of India has been issuing many guidelines to ensure that internet banking is functioning under a smooth basis and for the regulation and mitigation of the challenges of financial stability, information technology, technological risk management, cyber frauds. The Banking Regulation Act, 1949 does not deal with banking frauds directly but the provisions under this Act helps to understand the operations of banking sectors and the reasons behind the banking frauds that have occurred. Dr. K.C. Chakrabarty, the chairman and members of IIT, IIM, IDBRT, banks and Reserve Bank of India prepared the IT Vision Document 2011-2017 to increase the usage of internet banking. The competition has been very tough for the public sector banks as the newly established private sector banks and foreign banks are leaders in the adoption of internet banking. With lower internet costs and efficiency of internet, internet banking was started from 1999 in India.

The Information Technology Act, 2000 on online financial frauds

Cyber crime is any type of criminal activity that is carried out against individuals, against individual's property, against organization, against society at large to steal personal details, cause damage to electronic gadgets, harass, torture or defame people, thereby violating the right of privacy of netizens. The fraudsters make out different ways to steal personal information of netizens. For instance, they send emails or sms in the name of a bank or reputed company with an attached link. If we click on that link, fake website will open and will ask to provide card details, UPI Pin, OTP and other details and we may fall into the trap.[3] One of the most common all around the world on the internet is lottery fraud. The fraudsters send an email or whatsapp message by saying that a lottery worth crore has been won by the receiver.[4] Then there are some apps which ask people to deposit money for the registration of the app. Fraudsters create fake accounts or fake profiles on that app to cheat people. They will first make connections and affairs with the victim and act as innocent people and make up sad stories to ask people for money as a favor. There are few fake online shopping websites which display attractive products at the lowest price and offer discounts or cash back to gain the attention of the customers. Once the product is purchased and payment is done, either the product delivered is of cheap quality or not delivered at all. These websites also do not have any refund or return policy. These websites do not have cash on delivery as a payment method. Social media frauds are also very common all over the world. The fraudsters by making fake profile make contacts with people and induce them into online relationships. Then they gain their trust and ask for money or personal details. The recipients

[3] https://www.proofpoint.com/us/threat-reference/email-spoofing#:~:text=Email%20spoofing%20is%20a%20technique,users%20take%20at%20face%20value as on 03-04-2021

[4] http://www.cybercelldelhi.in/lotteryscam.html as on 03-04-2021

believing their profile to be real send money and fall victim of online financial fraud.[5]

In India, The Information Technology Act, 2000 deal with cyber crimes. The Act includes protection from cyber crimes like identity theft, cyber terrorism, hacking, cyber pornography, defamation, damage to computer or computer resources, etc. The provisions under IT Act dealing with internet financial frauds are as follows. Section 43 of the Act imposes penalty and compensation for access or securing access without permission, downloading or copying of data stored in a computer or computer resource, introducing computer viruses, damaging computers, denial of access, abetting such acts, illegal charging for services on another's account.[6] Section 66 of the Act makes a person liable for any act referred to in Section 43 and who does it dishonestly or fraudulently shall be penalized with detention for 3 years or with fine of 5 lakhs or with both.[7] Section 66B of the Act imposes a penalty with detention for a period up to 3 years or with fine of 1 lakh rupees or both for dishonestly receiving stolen computer resource or communication device.[8] Section 66C punishes an individual who makes use of the electronic signature, password or any other unique identification feature of any other person for a period of 3 years and will also be responsible for a fine which may extend up to 1 lakh rupees.[9] Section 66D of the IT Act penalizes a person who by means of any communication device or computer resource cheats by misrepresenting themselves. The offender shall be punished with imprisonment for a period of 3 years and shall also be responsible for a fine which may extend up to 1 lakh rupees.[10]

Analysis

The Act contains a lot of ambiguity and confusion. There is no provision on criminal breach of trust or misappropriation of property under the IT Act. The cyber crimes under this Act are always associated with the provisions under The Indian Penal Code, 1860. For example, data theft under section 43(b) read with Section 66 of IT Act is always associated Section 379, 420 of IPC, hacking under section 43(a) read with Section 66C of IT Act is associated with section 379 IPC, credit card fraud under section 43(a), 43(b) read with section 66 of IT Act is associated with section 420, 467, 468, 471 of IPC, dishonestly receiving stolen computer resource or communication device under section 66B is associated with section 413, 414 of IPC, phishing under section 43 of

[5] https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf as on 03-04-2021

[6] Section 43, Information Technology Act, 2000

[7] Section 66, Information Technology Act, 2000

[8] Section 66B, Information Technology Act, 2000

[9] Section 66C, Information Technology Act, 2000

[10] Section 66D, Information Technology Act, 2000

IT Act is associated with section 379, 420 of IPC, embezzlement, that is diverting money to one's own account can be explained under criminal breach of trust, misappropriation of property under the Indian Penal Code, 1860.[11] Section 379,413, 414, 420, 467, 468, 471 IPC includes punishment for theft, habitually dealing in stolen property, assisting in concealment of stolen property, forgery of valuable security, will, forgery for the purpose of cheating, using as genuine a forged document, respectively. The cyber crimes under the IT Act are bailable offences as a matter of right and it is only non-bailable when they are associated with the offences under IPC, which gives the offender an ample time to destroy the evidences when they are released on bail. Spam are uninvited and massive amount of emails where the recipient has not granted confirmable permission for the message to be sent and that the message is sent as a part of a larger collection of messages, all having similar content. The Information Technology Act, 2000 does not discuss the provision of spam at all. They should also have a provision to unsubscribe them or they may not be sent unless asked for. Australia has enacted the Spam Act which prohibits the sending of uninvited commercial electronic messages with an Australian link. In other words, commercial spam sent by phone or email is not permitted to originate from Australia and is not allowed to be sent by Australian addresses, whatever their place of origin. This will be enforced by the Australian Communications Authority. Many US States have enacted laws against unsolicited mail known as Anti Spam laws. The US Congress has enacted 'Controlling the Assault of Non-Solicited Pornographic and Marketing Act of 2003' or the 'CAN-SPAM Act, 2003' to solve these issues.[12] SPIM is an unavoidable or unrequested instant message. It has become an increasing threat to consumers. There is no specific law in India to deal with SPIM. The IT (Amendment) Act, 2008 reduced the quantum of punishment for a majority of cyber crimes. This needs to be rectified by enhancing the fines. The Act also does not cover a majority of crimes committed through mobiles. The Act thus becomes a weak legislation for the cyber criminals. Section 66C of IT Act defines identity theft to be an offence but does not mention frauds committed without using electronic signatures or unique identification features. Thus identity fraud is often but not necessarily the consequence of identity theft. Someone can steal or misappropriate personal information without committing identity theft using the information about every person, for instance when a major data breach occurs.[13] The increasing internet financial frauds highlight the need to set up a broader regulatory framework to protect our technological sovereignty. The Information Technology Act, 2000 also

[11] The Indian Penal Code, 1860

[12] https://spamlaws.com/world.shtml as on 28-04-2021

[13] https://en.wikipedia.org/wiki/Identity_theft as on 28-04-2021

does not speak about data security and data privacy. Therefore, India needs to have a modern and specific legislation on digital money transactions so that data breaches do not occur while making a digital payment. The lack of any specific regulatory framework gives chance to scammers to steal personal data.

Result of the empirical study[14]

To study the opinion of netizens on online financial transactions, a survey has been made based on some questions which are as follows-

Table 1 : Opinion given by the netizens of Kolkata (Total No. of respondent :45)

Sr. no.	Questions	Yes (%)	No (%)
1.	Are you aware of The Information Technology Act, 2000?	92.82	7.18
2.	Did you ever receive any message which said that you have won a lottery and then called you to share your bank details?	81.78	18.22
3.	Did you ever receive any fake messages, emails or calls representing them to be from reputed companies and asked you to share your bank details, password, OTP, PIN etc?	98.20	1.8
4.	Have you ever invested any money for registering an app and afterwards found that app to be a fake one?	47.33	52.67
5.	Do you think a modern and specific legislation is needed to deal with the emerging frauds on online financial transactions?	100	0

From the age 21-65, both male and female respondents gave their opinion on online financial transactions. Table 1 demonstrates the data analysis of the respondents within the study area. The result of table 1 is further shown in the figure 1.

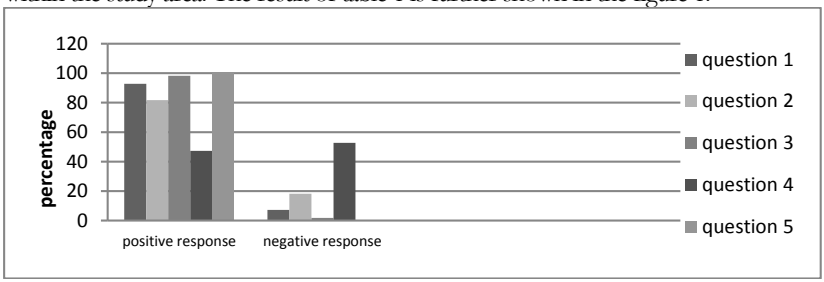

Figure 1 : Pictorial demonstration of the viewpoint of the respondents

Figure 1 represents the viewpoint of the respondents on online financial transactions which has been calculated in percentage. It shows both the positive responses and the negative responses of the respondents within Kolkata based on the questions asked by the author.

Suggestions

Here can be some measures to protect the confidentiality and privacy of personal data of netizens whenever they are making any online money payment.

Smart and cautious use of internet by the netizens, OTP, password, PIN, CVV, other bank details should not be shared with any anyone, Do not click on any unverified links sent by unknown and suspicious email addresses or instant messages, Should not download unpopular apps because that can

[14] Source: author

contain malware or virus, Unknown public wifi should not be used because that can lead to hacking, Two-step verification should be enabled on all apps by the users so that if anyone hacks, a security alert will be shown, Before registering for an app, verify whether it is real or fake, All permissions to access by an app should be removed once that app is downloaded, Last login should be checked, First Information Report (F.I.R.) or General Diary (G.D.) should be lodged by the victim within three days to recover the lost money, Global awareness of the right of netizens, Strong enforcement mechanism for the protection of the rights.

Conclusion

Thus it can be concluded from the above study that the frauds on e-banking has increased, especially during the pandemic. Online transactions are effortless, saves time and cost without much hassle making digital frauds a common occurrence. By questioning people of different ages, it can be inferred that fraudsters are always trying to find an opportunity to steal people's money by various ways. The netizens should be extra cautious of their technology rights and know how to handle their personal data. In my opinion, it is better to use bank's personal net banking app or website while making any online transaction rather than any outsider app, though all third party apps are not hoax. In that case also we have to remain alert by not sharing any OTP, PIN, password to any bank employee and we should always verify an app before registering for it. Though there are sufficient laws on online financial frauds which to some extent help prevent the frauds, a strong and specific legislation is needed in India to deal specifically with the financial frauds digitally. The Information Technology Act, 2000 is always dependent on The Indian Penal Code, 1860 to forbid the occurrence of digital money frauds. The Indian Penal Code, 1860 does not define the word 'fraud' entirely and does not specifically mention the classification of digital money frauds. Therefore, a specific legislation is the need of the hour to keep pace with the emerging technologies and issues on digital financial frauds. Global awareness, education of promotion of the rights of the netizens is also needed to stop the occurrence of frauds.

References

Justice Yatindra Singh, Cyber Laws, 4th edition, Universal Law Publishing Co. Jyoti Rattan, Cyber Laws & Information Technology, 6th edition, 2017, Bharat's

K. D. Gaur, The Indian Penal Code, 4th edition, Universal Law Publishing Co.

Babu Sarkar's, Information Technology and Cyber Crime Law in India, 1st edition, 2014, Moon Law Agency

Chandrawati NIrala, Dr, BB.Pandey, 'Evolution of e-banking in India- An Empirical Study'

https://spamlaws.com/world.shtml

The Times of India