E BANKING AN INTEGRAL PART OF THE BANKING SYSTEM- A LEGAL OVERVIEW

Bhaswati Borah
Research Scholar, RSLA, The Assam Royal Global University, Guwahati
Assistant Professor, NEF Law College, Guwahati

Abstract

E-banking, sometimes referred to as digital banking, internet banking, or online banking, is a system that makes it possible to conduct financial activities online, such as money transfers, loan and EMI payments, cash deposits, and cash withdrawals. In today's world, e-banking makes a significant impact to economic growth, especially in emerging nations like India. The focus of banks has changed from conventional banking to the digital banking system. E-banking is a rapidly expanding idea in the banking industry. The banking business has seen a significant beneficial transformation due to technological innovation. It makes it possible for anybody, anywhere to conduct financial transactions at any moment. However, there is a drawback to online banking. It isn't completely safe. A significant sum of money is moved illegally through e-banking scams. The expansion of information technology has led to a new form of banking. Traditional banking, based on the physical presence of the customer, is only a part of banking activities. In the last few years, electronic banking has emerged, adopting a new distribution channels like Internet and mobile services. The main goal was to allow businesses to improve the quality of service delivery and reduce transaction cost, and anytime and anywhere service demand for customers. However, it increased the vulnerability to fraudulent activities like spamming, phishing and credit card frauds. Then, the main challenge that opposes electronic banking is ensuring banking security most importantly legal preventive measures are required to curb this menace.

Keywords- e banking, digital banking system, traditional banking

A significant sum of money is moved illegally through e-banking scams. A poor ordinary man makes great efforts to save money for emergency situations, but e-banking fraudsters employ every malfeasance to make money quickly and steal from the poor. There are laws in place to regulate it. True evidence of it may be found in the Information Technology Act of 2000. In addition to that, the Reserve bank also promptly releases instructions in this respect. In order to address these serious concerns, a separate complaint cell has been developed. However, it has been shown that these offences are becoming worse every day. Therefore, it is important to research it and identify a workable solution to this problem. The examination of the relevant legislation and their critical analysis has been the main subject of the researchers' work. In addition to that, the yearly reports of the relevant agencies, including the National Crime Report Bureau and the Internet Crime Complaint Centre, have also been read. The judiciary has also been paid proper attention to it. After going through all available material, the researchers have supposed to recommend some suggestions to carry on e-banking in a more effective an

Factors of Banking Fraud In E-Banking

The actors of banking fraud can be categorized into four main categories; malicious exploiters, money mules, victims, and security guardians. Each of these actors and their characteristics have been defined below individually.

Cyber Criminals

As per the OECD report (2007)[1], these malicious exploiters can be categorized into five sub categories. ***Innovators*** (who seek to find security holes in the system to overcome protection measures adopted by the banks), ***Amateur*** (who are beginners in this area and their expertise is limited to computer skills, which is exploited by the cyber criminal), ***Insiders*** (who are working within the bank to leak out important information in order to take some kind of revenge). ***Copy cats*** (they are interested in recreating simple tasks). ***Criminals*** (highly organized and very knowledgeable who may use all the above mentioned stakeholders for their own profit).

Money Mules

As per the definition given by OECD report (2007), money mules are individuals recruited wittingly and often unwittingly by criminals, to facilitate illegal funds transfers from bank accounts. According to the FBI (Federal Bureau of Investigation), these individuals engage in the money transfer activity in exchange of some percentage of that money. According to Florêncio and Herley (2010)[2] there role is to convert

[1] OECD. 2007. Malicious Software Malware: A Security Threat to the Internet Economy.
[2] Florêncio, D., & Herley, C. 2010. Phishing and money mules. In Information Forensics

reversible traceable transactions into irreversible untraceable ones.

Victims

Victims, according to OECD (2007)[3], in the banking sector can be categorized into two categories; banks and users of these banks. The users or customers can be individuals, SMEs, or large multinational organizations. The most negative externality among the legitimate actors is created by individual users and SMEs who do so by not employing risky online behavior or by not employing security measures during transactions (Asghari, 2010[4]; Mannan & van Oorschot, 2008[5]).

Security Guardians

They are the most important actor of this system as they improve the existing banking system and help in removing the vulnerabilities and development of systems so that banking frauds can be mitigated. The security guardians in case of banking sector could be the bank itself or the some third party hired by the bank in order to ensure security from such threats.

Impact of Crime/Offences/Frauds Related To E-Banking On Banks

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions. The banking sector is forced to evaluate its current practices in order to analyze and manage their risks effectively. Technology-driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in everyday life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services affordable and accessible (KPMG, 2011)[6].

However, this has also increased the risk of becoming targets of cyber attacks. Cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the bank s finances. Globally, USD 114 Billion is lost nearly every year due to cybercrimes, and the cost spend to combat cybercrimes is double is amount i.e. USD 274 billion (Symantec Cyber Crime Report, 2012)[7].

On an average, banking facilities take 10 days to fully recover from a cyberact which further adds to the cost of operation. Comparing the financial losses faced by the Indian Banking Sector, it is nearly 3.5% of the loss in cash in comparison to global loss. USD 4 billion is lost in recovering from the crime and USD 3.6 billion is spent to combat such crimes from happening in future. The average time taken to resolve the crime in Indian banking sector is also higher in comparison to global scenario i.e. 15 days (Muthukumaran B., 2008)[8].

In order to fight these cybercrimes, the banking sector needs to collaborate with global authorities and watchdog organizations so that a model can be developed which can help in controlling and dealing with such threats. The main issue of concern here is that there is absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks (Stafford, 2013)[9].

High profile banks in the UK like Barclays and Santander were targeted by hackers who stole personal information of nearly 2.9 million credit card customers by hacking the software maker system of these banks, which led them to incur huge losses. However, the scenario is not restricted to UK, in US as well such attacks have surfaced in the past years and in order to curb the affect, they launched the program Quantum Dawn 2 which test

and Security WIFS, IEEE International Workshop on pp. 1-5. IEEE.

[3] OECD. 2007. Malicious Software Malware: A Security Threat to the Internet Economy.

[4] Asghari, H. 2010. Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity. Delft University of Technology.

[5] Mannan, M., & van Oorschot, P. C. 2008. Security and usability: the gap in real-world online banking. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms.

[6] KPMG 2012 [Online] Cybercrimes: A Financial Sector Review. Government and Public Sector. Available at: https://www.kpmg.com/in/en/industry/publications/fs_cybercrime_booklet.pdf

[7] Symantec Cyber Crime Report, 2012 [Online] Cybercrime Report. Available at: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport. pdf

[8] Muthukumaran. B 2008. Cyber Crime Scenario in India, Criminal Investigation Department Review, pp.17-23

[9] Stafford P. 2013 [Online] Cyber crime threatens global financial system. Available at: http://www.ft.com/cms/s/0/9804988c-3722-11e3-9603-0144feab7de.html.

the efficacy of system installed in banks in response to cyber-attacks (Stafford, 2013)[10].

However, the sad truth is that most the systems are one-step behind the tools adopted by cyber criminals which has resulted in demand of development of system which is flexible is meeting and destroying the incoming assaults. A solid defense system to resolve attack is the need of the hour before, during and after the attack.

In developing economies, cybercrime has increased rapidly due to high usage of the internet and the digitization of economic activities. Need of strict statutory laws to regulate the criminal activities in the cyber world was needed which should also aim to protect technological advancement system as the misuse of technology was increasing at a very high rate. To control these fraudulent practices Indian parliament made "Information Technology Act, 2000" on 17th Oct 2000 which deals with the laws in the field e-commerce, e-governance, e-banking as well as fines and punishments to be imposed with to control cybercrimes. Cyber Crime may be stated as "unlawful acts wherein the computer is either a tool used to perform the crime or it becomes a target of crime or sometimes both."[11]

Cyber Crime is neither defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008. Under the Indian Penal Code, 1860 and a few other legislations meaning of crime or offence has been elaborated which is not done in this act. Hence, to define cybercrime, we can say, it is just a combination of crime and computer. To put it in simple terms "any offence or crime in which a computer is used is a cyber crime".

Certain Acts of Information Technology Act -2000 and the I.T. Amendment Act 2008 were enforced with reference to banking and financial sector transactions. During mid of 90‟s India saw an improvement in globalization and computerization, growth of computerized governance and growth in E commerce was witnessed during this period. Until then, most of international trade and transactions were done through documents being transmitted through post only. Documentary evidences & records were mainly paper evidences and paper records or other forms of hard-copies only. As international trade was mostly being done through electronic communication and emails, an urgent need for maintaining and storing electronic records was realized.[12]

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes various cyber crimes related to electronic/internet/digital banking.[13]

- Cracking: It is one of the most alarming cyber crimes. In this case offender can damage inside our computer systems without our knowledge and permission and can make unauthorized alterations in precious confidential data and information.
- E-Mail Spoofing: A spoofed e-mail is the one which misrepresents its origin. It shows different origin not from where actually it has originated.
- SMS Spoofing: Spoofing is a blocking through spam ("spam" means the unwanted and uninvited messages). In this case offender steals identity of another person in the form of mobile phone number and sends SMS via internet and receiver gets the SMS from the mobile phone number of the victim. SMS spoofing is a serious cyber crime against any person.[14]
- Carding: It means making false ATM cards (i.e. Debit and Credit cards) which are used by criminals for their monetary benefits for the purpose of withdrawing money from the victim's bank account without his knowledge and faith. More of the unauthorized use of ATM cards is seen this type of cyber crimes.
- Cheating & Fraud: Person who tries to steal password and data storage does it with a negative mind which leads to fraud and cheating.
- Assault by Threat: This category refers to threatening a person with for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

[10] Stafford P. 2013 [Online] Cyber crime threatens global financial system. Available at: http://www.ft.com/cms/s/0/9804988c-3722-11e3-9603-0144feab7de.html.

[11] Ajeet Singh Poonia, cybercrime, challenges and its classification, International journal of Emerging Trends and Technology in Computer Science (Volume 3,issue 6, Nov- Dec 2014,pg 120)

[12] Ajeet Singh Poonia, cybercrime, challenges and its classification, International journal of Emerging Trends and Technology in Computer Science (Volume 3,issue 6, Nov- Dec 2014,pg 120)

[13] Kamini Dashora, Cyber Crime in the society: Problems and Preventions, 2011,vol-3,pg 243-244.

[14] Kamini Dashora, Cyber Crime in the society: Problems and Preventions, 2011,vol-3,pg 243-244.

- Intellectual Property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which owner is deprived completely or partially of his rights is an offence. The general forms of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.[15]
- Online Gambling: Online fraud and cheating has now become money making business which is growing presently in the cyber world. There are many cases which reveal credit card crimes, fake job offerings, etc.
- Financial Crimes: Users of networking sites and phone networking try to attack the victim by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.[16]
- Forgery: To cheat and deceive large number of persons by sending threatening mails as online business transactions and troubling the victims is increasing at a large speed.
- URL hijacking or squatting: Using the domain name in bad faith. The squatters neglect the existence of a trademark to profit from others. Same Domain name claimed by two parties either by claiming that they had registered the name first or by right of using it before the other. Typo squatters will buy a domain with a typo in them. For example two similar names i.e. www.yahoo.com and www.yaahoo.com. or www.linkdin.com or www.linkedin.com.[17]
- Cyber Vandalism: Vandalism means purposefully or intentionally destroying or damaging property of another. Cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.[18]
- Hacking Computer System: Hacking refers to unauthorized access/control over the computer which results in loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and are done to damage the reputation of particular person or company.
- Virus transmission: Viruses are programs that attach themselves to a computer or a file and then circulate and infect other files and other computers on a network. The data on a computer is affected by them either by altering or deleting the data from the system.[19]
- Unauthorized access or Trespass: Accessing someone's computer without the right authorization of the owner without disturbing, altering, misusing, or damaging data or system by using wireless internet connection.[20]
- Internet Time Thefts: Internet time theft comes under hacking. An unauthorized person uses the internet for his own usage and number of the Internet hours is paid by another person. Victim‟s ISP user ID and password is accessed by unauthorized persons, either by hacking or by gaining access to it by illegal means and he uses it to access the Internet without the other person‟s knowledge. One can identify time theft if internet time (hour) has to be recharged often, despite infrequent usage.
- Cyber Terrorism: Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.[21]
- Cyber Warfare: Cyber warfare involves the battle space use and targeting of computers and

[15] McCullagh, A., & Caelli, W. 2005. Who goes there? Internet banking: A matter of risk and reward. Paper presented at the Information Security and Privacy.

[16] Ibid

[17] Muthukumaran. B 2008. Cyber Crime Scenario in India, Criminal Investigation Department Review, pp.17-23

[18] Ibid

[19] Premchaiswadi, N., Williams, J. G., & Premchaiswadi, W. 2009. A Study of an On-Line Credit Card Payment Processing and Fraud Prevention for e-Business. In T. Bastiaens, J. Dron, & C. Xin Eds., World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2009: 2199-2206. Vancouver, Canada: AACE.

[20] Digpal Singh, H Rathore and Karn Marwah: Cyber Crime in Banking Sector .International journal of law mantra. www.lawmantra.co.in.www.cyberlawsindia.net

[21] Premchaiswadi, N., Williams, J. G., & Premchaiswadi, W. 2009. A Study of an On-Line Credit Card Payment Processing and Fraud Prevention for e-Business. In T. Bastiaens, J. Dron, & C. Xin Eds., World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2009: 2199-2206. Vancouver, Canada: AACE.

networks in warfare. It involves both offensive and defensive operations pertaining to the threat of cyberattacks, damages, disruptions and sabotage.

- Distribution of pirated software: It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- Possession of Unauthorized Information: It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Cyber Crimes affects the companies at large as almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security threats and risks. In the modern cyber world cyber crimes is the major issue which is harming an individual as well as society at large.[22]

Legal Protection Mechanism For E-Banking In India

Government of India enacted its Information Technology Act 2000 with its objectives stated in Act itself "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the deserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto." The Information Technology Act, 2000, was thus passed as the ctNo.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000.The Act mainly deals with certain issues like legal recognition of electronic documents, legal recognition of digital signatures, offenses and contraventions, justice dispensation, systems for cyber crimes.[23]

Amendment Act 2008

The previous Act was the subject of certain debates, reviews and few criticisms. Due to some omissions in the act it resulted the investigators to rely more and more on the provisions of Indian Penal Code even in technology based cases with the I.T. Act ITACT was referred but reliance was more on IPC rather on the ITA. The need for an amendment was felt for the I.T. Act from the year 2003-04. Major industrial bodies were consulted and advisory groups were formed to suggest recommendations for the need of Information Technology Amendment Act 2008. This Amendment Act got the President assent on 5th Feb 2009 and was made effective from 27 Oct 2009. ITAA considers main issues like data privacy, information security, defining cybercrime, making digital signature technology neutral, defining reasonable security practices to be followed by corporate, redefining the role of intermediaries, recognizing the role of Indian Computer Emergency Response Team, inclusion of some additional cyber crimes like child pornography and cyber terrorism, authorizing an Inspector to investigate cyber offences (as against the DSP earlier).

Penalty For Damage To Computer System: According to the Section: 43 of "Information Technology Act, 2000" whoever does any act of destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine up to 1crore to the person so affected by way of remedy.[24] According to the Section:43A which is inserted by "Information Technology (Amendment) Act, 2008 where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with

[22] Premchaiswadi, N., Williams, J. G., & Premchaiswadi, W. 2009. A Study of an On-Line Credit Card Payment Processing and Fraud Prevention for e-Business. In T. Bastiaens, J. Dron, & C. Xin Eds., World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2009: 2199-2206. Vancouver, Canada: AACE.

[23] Mannan, M., & van Oorschot, P. C. 2008. Security and usability: the gap in real-world online banking. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms.

[24] Mannan, M., & van Oorschot, P. C. 2008. Security and usability: the gap in real-world online banking. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms.

„hacking with computer system" and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Preventive Measures

Certain measures are taken by users while using the internet to perform digital banking transaction which will help them to combat the Cyber Crime is not to reveal their account details via e-mails and while chatting. Updated Anti-virus software protection against virus attacks should be used by all those who are using internet. One should never reveal credit card number to any unsecured site to guard against frauds. Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day. It is better to use a security programmes by the body corporate to control information on sites. Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of customers. Justice must be provided to the victims of cyber crimes. They should be provided compensation and offenders are also to be punished.[25]

With the increasing use of internet services worldwide, it is becoming easy to access any information easily.[26] Internet which is the medium for huge information and a large base of communications but using it can be beneficial if certain precautionary measures are also taken by users while using the internet which will help them to combat the Cyber Crime.

- Abhijit V. Banerjee, Shawn Cole, and Esther Duflo, ‘Banking Reform in India’, Department of Economics, MIT, NBER and CEPR, 2004
- Acharya, Shankar, ‘Indian: Crisis, Reforms and Growth in the Nineties; working paper No. 139, standard University, 2002
- Ajeet Singh Poonia, cybercrime, challenges and its classification, International journal of Emerging Trends and Technology in Computer Science (Volume 3,issue 6, Nov- Dec 2014,pg 120) Banerjee, Abhijit and Esther Duflo, ‘Efficiency of lending operations and the impact of priority sector Regulations’, MIMEO, MIT, 2000
- Bartel, A. P. “Human Resource Management and Organizational Performance: Evidence from Retail Banking”. Industrial and Labor Relations Review, 57(2): 181-203, 2014.
- Benedikter, R. “Answers to the Economic Crisis: Social Banking and Social Finance”. Spice
- Florêncio, D., & Herley, C. 2010. Phishing and money mules. In Information Forensics and Security WIFS, IEEE International Workshop on pp. 1-5. IEEE.
- Florêncio, D., & Herley, C. 2011. Where Do All The Attacks Go? Economics of Information Security and Privacy III pp. 13-33. Springer New York
- Kamini Dashora, Cyber Crime in the society: Problems and Preventions, 2011,vol-3,pg 243-244.
- KPMG 2012 [Online] Cybercrimes: A Financial Sector Review. Government and Public Sector. Available at: https://www.kpmg.com/in/en/industry/publications/fs_cybercrime_booklet.pdf
- Muthukumaran. B 2008. Cyber Crime Scenario in India, Criminal Investigation Department Review, pp.17-23
- OECD. 2007. Malicious Software Malware: A Security Threat to the Internet Economy. Sankar. R, ‘The Financial Sector: Vision 2020’, Academic Foundation, New Delhi, 2003.
- Satish Munjal, ‘Banking Operations’, Print well Publishers, Jaipur, 1990.
- Saxena, N. and Monika, K. “Organizational Culture and its Impact on Employee Retention”. Pacific Business Review, 2(3): 102-110, 2010

[25] Ibid

[26] Ibid