International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 01, January - March, 2021, pp 282-286

LEGAL MECHANISM OF CYBER CRIMES AGAINST E-BANKING IN INDIA

Dr. C.P. Gupta[*]
Abhilasha Sharma[**]

ABSTRACT

Banking system is one among the oldest businesses systems in the world and retained its existence from earlier period in India. The banking industry has its source in the earlier centuries. Awareness of banking was there among the prehistoric society because they felt the requirement of banking and makes use of cash transaction to induce proper benefits. The importance of banking industry was recognized by the people because they'd realized the worth of cash in their life. Application of data Technology was successfully administered in the industry. Maximum banking transactions were done through information technology. Therefore it's concluded that information technology is the trouble shooter of the industry and also most helpful for the shoppers for his or her day to day banking transactions. Phone Banking, automated teller machine Machines (ATM), Credit Cards, Debit Cards, ATM Cards, Smart Cards, Electronic Funds Transfer (EFT), Shared Payment Network System (SPNS), Electronic Clearing Services (ECS), Point of sale [POS] terminal, D-Mat Accounts, Electronic Data Interchange (EDI), E-Cheques, Computerized Accounting, E-Mail and RBI Net are a number of the samples of administration of knowledge Technology in the Indian banking industry. However the implementation of recent technology in banking system and advancement of E-banking not only offered opportunities for the shoppers to avail comfortable banking services and for the banks to expand banking business but has also gave an equal opportunities and opened the doors for brand spanking new criminal activities. The current research work is the assessment of the impact of cyber crimes on the E-banking in India. This study is a trial to search out up to what extent legal provisions are effective and efficient enough for controlling the cyber crimes against e-banking in India. The results of this study may encourage be helpful in assessing the effectiveness of the legislation, their weaknesses and can suggest ways to amend and plan for the longer term.

Keywords: *Banking, Banking system, Criminal Activities, Cyber Crimes, Information Technology.*

Introduction

Banking industry has capable major changes in recent past. Most the banks in India have adopted Information Technology solutions for rendering the banking services to their customers by using the IT tools & techniques to meet the requirements of the purchasers. Due to the dawn of e-banking, conventional banking has been disappeared from the Indian banking scenario and banks have shifted from traditional banking to Core Banking Solution. However the technology that facilitated bank and its customers to perform business more effectively also provided the opportunities of worldwide organized criminal networks. Due to advancement of data and communication technology the complete world is transformed into a world village but at the same time it put a heavy threat to the present and established banking institutions called “Cyber Crimes”. The event of data Technology (IT) introduced the cyber space wherein internet made available equal opportunities to any or all the people to access any information and data storage. Because of increase of internet users, misuse of technology within the cyberspace was take hold of cyber crimes at the domestic and international level. “Cyber crime” is an criminal activity committed by using the pc or other electronic devices or Internet because the medium, in violation of

[*] Research Supervisor, Head & Associate Professor, Faculty of Law.
[**] Research Scholar, Faculty of Law, Jagannath University, Jaipur, Rajasthan, India.

existing enactment that punishment is awarded as per the statute of the country. The world nature of engineering presents a challenge to the nations in the world to deal with Cyber crime. Domestic solutions are inadequate because cyberspace has no geographic or political boundaries, and plenty of computer systems may be easily accessed from anywhere in the world. It's also difficult to get accurate Cyber crime statistics because many of the incidents weren't reported and lots of of the incidents were even not detected. Cyber crimes are increasing globally and India too has been witnessing a pointy increase in cyber crimes in the recent years.

Objective of Study

The objectives of this research work are to the touch all the important facets of the legal control of cyber crimes against e-banking in India during a comprehensive way and to realize new insights into it. The main objectives of this study are as under:

- To check the meaning & concept of cyber crimes specifically related with E-banking.
- To check the offenses related with cyber crimes specifically related with E-banking in India.
- To review the issues of law to regulate the cyber crimes against E-banking in India.
- To gauge the importance of assorted existing national and international laws related with e-banking in India.
- To means the loopholes in the existing national laws to regulate the cyber crimes against e-banking in India.

Legal provisions are proving insufficient to regulate of Cyber Crimes and providing remedies to the purchasers & banking institution. Moreover, the present national laws aren't sufficient to accommodate the domestic e-banking transactions. Therefore this study will throw light on the insufficiency of legal remedy for e- banking and can suggest where the complete proof amendments in legal provisions are required to facilitate legal control of cyber crimes against e- banking in India.

Review of Literature

Tewari R.K, Sastry P.K and Ravikumar K.V. in their book "Computer Crime and Computer Forensics" the author describes the pc Networking and therefore the Internet. He further discussed the Vulnerabilities of Computer Networks. The author described the emergence of Computer Crime and also the Internet Crimes and Network Security Measures. He commended on Digital Signatures and Cryptography. He discussed the National and Int6ernational coordination to handle the cyber crime.

S.B.Verma, S.K. Gupta & M.K. Sharma in their book "E-Banking and Development of Banks" described the final history of banking. The Authors further described the adoption of IT in banking has undergone several changes with the passage of time. Today it's become an inseparable segment of banking organization. The appliance of data technology within the banking sector resulted within the development of various concepts of banking like – E-banking, Internet Banking, Online Banking, Telephone Banking, machine machine, universal banking and investment banking etc.

Nandan Kamath in his book "Law referring to computers, Internet and E-Commerce (A guide to Cyber Laws and therefore the Information Technology Act, 2000)," the author commented on the cyberspace because it becomes a money spinner and it'll increasingly become the domain of business legal & illegal. As a possible information technology power, India should take warning from the hunting hackers and put the system wary. The author also discussed the importance of electronic evidence in the case of cyber crimes. He further added about the legitimacy of the electronic records to be produced as electronic evidence. He exhaustively explained about the burden of proof associated with electronic evidence.

Rupa Mehta and Rohinton Mehta in their book "Credit Cards a Legal Guide" with special relation to credit card Frauds, the authors described the proliferation of credit cards in our daily lives and also the billion dollars of fraud perpetrated using credits. The authors commented on Money and Plastic Money, forms of Cards, Smart Cards and features of Cards. He explained the card board Cycle. They further discussed credit card Fraud and Fraud detection techniques. They explained credit card Fraud Investigation techniques. The authors further commented on Credit Cards and legal code and therefore the Liability of Banks & Card holder.

Justice Yatindra Singh in his book "Cyber Laws" has described the adoption of IT in banking has undergone several changes with the passage of time. the applying of data technology in the banking sector resulted within the development of various concepts of banking like – E-banking, Internet Banking, Online Banking, Telephone Banking, automated teller machine machine, universal banking and investment banking etc. Information technology includes a lot of influence on banking transactions. He further threw light on trademarks, copyrights, patents & their existence in cyber space.

Baibridge D. in his book "Introduction to Computer Law", the author described the cyber frauds, its definition and kinds of the cyber frauds. He also described the ATM frauds and Card Trapping Attack. Skimming Attack, Phishing/Vishing Attack, Pin Cracking Attack, ATM Hacking. ATM Malware Attacks, Carders, the people that buy, sell, and trade online the credit card and Internet Search Engine/Google "Hacking".

Rational of Study

As the cyber crimes incidents against e-banking are increasing day by day therefore this study requires examining the impact of legal control of cyber crime against e-banking in India. Cyber laws of the nations are enacted to test and control the cyber crimes incidents against e-banking. If the cyber laws of the country are enough competent and efficient to test and control the cyber crimes then there's no growth/ or controlled growth in the cyber crimes. Statistical data of state organizations like bank of India (RBI), National Crime Record Bureau (NCRB), and Indian Computer Emergency Response Team – India (CERT In) published on their official website has been collected and employed in this study. Similarly, annual publication by RBI on Banking and Finance, Quarterly RBI Bulletins, Publication of Indian Banks Association Chartered Accountants of India and Government of India is additionally consulted during this study.

Research Methodology

The methodology is mostly a suggestion system for solving an issue, with specific components like phases, tasks, methods, techniques and tools. In simple word it describes the way the research has been administered. It includes overall research design, setting objectives, the format for data collection, the info collection method, the sample design, the many tools and techniques won't to present the knowledge and last but not the smallest amount the analysis procedure.

Source of Data

The study is entirely supported the secondary data and published data by the government and government agencies. The Publication of the banking concern of India, Indian Banks Association, Indian Computer Emergency Response Team – India (CERT In), Press Information Bureau of India, Ministry of Finance publications and Government of India publications provide source of trustworthy and authentic data of the secondary nature.

Data Analysis

The secondary data collected from authentic sources just like the RBI, CERTIn (Computer Emergency Response Teams India) et al. are arranged during a series and analyzed the information by using percentage to match a series of information to explain the link among the variables.

Results and Analysis

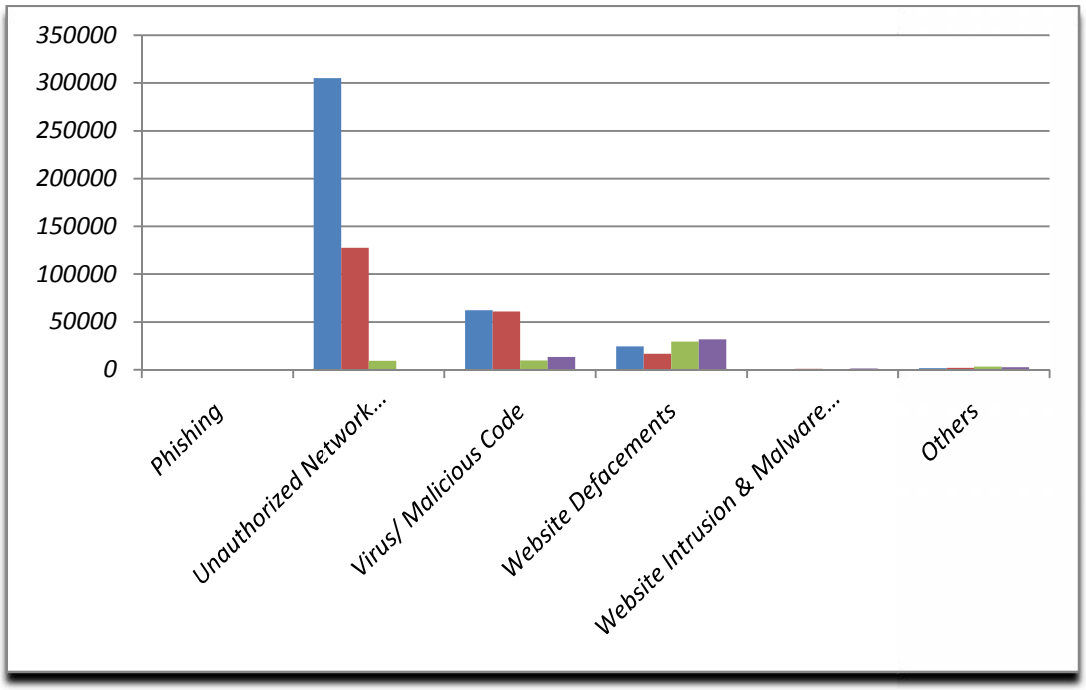
As per Certin, following Data as shown below indicates the total incidents of various types of Crime crimes undertaken in up to year 2019.

As we can see in the table, the cyber crimes are increasing every year. With the increased use of Technology, and internet, the cyber crime is increasing and not proportionally but more than that. As shown by the table, Unauthorized Network Scanning/Probing/Vulnerable Services has increased drastically. With compare to 2018, it was more than double in 2019. Same has Website Intrusion & MalwarePropagation has decreased in 2018, but again increased in 2019. However it is less compare to 2017 and 2016. The Virus/ Malicious Code increased with drastic rate. Compare to 2017 it 63163 in 2019 amounting to around 6 times of 2017. Only Phishing and Website Intrusion & MalwarePropagation have shown a decreasing trend and it is observed that they have been controlled or may be possible that they converted into other kind of frauds.

Table 1: Cyber Crimes in India

Security Incidents	2019	2018	2017	2016
Phishing	472	454	552	757
Unauthorized Network Scanning /Probing/Vulnerable Services	305276	127481	9383	416
Virus/ Malicious Code	62163	61055	9750	13371
Website Defacements	24366	16655	29518	31664
Website Intrusion & MalwarePropagation	417	905	563	1483
Others	1805	1906	3351	2671
Total	394499	208456	53117	50362

Chart 1: Security Incidents



Legal Remedy Available for Cyber Terrorism under I.T. Act, 2000

The threat created by the malware for cyber terrorism is successfully controlled provided that provisions of the I.P.C with the strict provisions of the data Technology Act, 2000 jointly implemented. Courts can use their discretion by combining provisions of assorted statutes to try and do the entire justice goodbye the provisions can operate in the presence of every other. Accordingly, the Indian legal code, 1860 and also the provisions of IT Act is add-on with the provisions of I.P.C to manage the cyber terrorism. The protection of IT Act is claimed for:

- Violations of Privacy: Right to privacy could be part of the proper to life and private liberty enshrined under Article 21 of the Constitution of India. The assorted provisions of the IT Act 2000 pertinently protect the web privacy rights of the netizens. The legal remedy available against the culprit using the malware. Section 1(2) read with Section 75 of the IT Act 2000 provides for an extra-territorial application of the provisions of the Act. Thus, if someone (including a far off national) contravenes the privacy of a personal by means of computer, system or network located in India, he would be liable under the provisions of the IT Act 2000.
- Prevention of data and data theft: Provisions of IT Act 2000 handling the information theft under section 43, section 65, Section 66, Section 70 and Section72 may be successfully invoked. Likewise Provisions of ITA Act 2008 under section 43A and section 72A jointly supplemented with section 22 of I.P.C.,1860 and 378 of I.P.C.,1860 will be invoked.
- Prevention of distributed denial of services attack: A malware can also use the strategy of distributed denial of services (DDOS) to overburden the electronic bases of people. Thus, distribute denial of services by use of malware are going to be tackled by invoking the provisions of sections 43,section 65 and section 66 of IT Act 2000 collectively.
- Prevention of network damage and destruction: In India there's no law, which is specifically coping with prevention of malware through aggressive defense. Thus, the analogous provisions must be applied in an exceedingly purposive manner.

Conclusion

Banks are considered as the most reliable and responsible institution in managing the finances and money matters. A banking organization is the key to economic process and development of the country. Financial & social reforms were applied in the banking sector in India after independence. As a

motto in criminology goes “a crime will happen where and only the chance avails itself.” Until recently, we were awake to only traditional styles of crimes like murder, rape, theft, extortion, robbery, dacoity etc. But now with the event and advancement of science and technology there came into existence machines like computers and facilities like internet. The internet has displayed a full new virtual heaven for the people good and bad, clever and naive to enter and interact with lot of diverse cultures and sub-cultures, geography and demographics being no bar. The exact same virtues of internet when gone in wrong hands or when exploited by people with dirty minds and malicious intentions, make it a virtual hell. As a results of the rapid adoption of the net globally, computer crimes are multiplying like mushrooms. At the identical time, the legislators face the requirement to balance the competing interests between individual rights like privacy and free speech, and also the must protect the integrity of the world’s public and personal networks.

References

- ✓ Haq S and Khan B.L.“ E-Banking Challenges and opportunities in The Indian Banking Sector” published in Innovative Journal of Business and Management 2 : 4 July – August (2013) available at www.innovativejournal
- ✓ Jagadeesh, S. (2005) “Credit Card Fraud: Causes and cures from professional’s perspective. C.A Journal of the Institute of CAI, Vol. 53 No. 7, January.
- ✓ Malik, V. Value reporting and Global comparative advantage (Banking and Finance), VMA Information Pvt Ltd, New Delhi, 2005
- ✓ Manikyam K.Sita Mrs. “Cyber Crimes Law & policy perspectives” published by Hind Law House Pune. 2009.
- ✓ Nandan Kamath, Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Universal Law Publishing Co., 2009.
- ✓ R.K. Chaubey, An Introduction to Cyber Crime and Cyber Law, Kamal Law House Publication, 2009
- ✓ Radhakrishna Geeta and and Point on Leo, “Fraud in Internet Banking: A Malaysian Legal Perspective”, ICFAI University Journal of Bank Management, Vol. VI, issue 1 (Feb. 2007)
- ✓ Research paper “DETECTION OF CYBER CRIMEAND INVESTIGATION” presented by Justice K.N.BASHA, Judge, Madras High Court, Chennai, in the Seminar and Workshop organised on 28.06.2010 & 29.06.2010 at Sardar Vallabhbhai Patel National Police Academy, Hyderabad
- ✓ Reserve Bank of India “Anti-Money Laundering (AML) Measures/Combating of Financing of Terrorism (CFT)/Obligations of banks under PMLA, 2002” – 30th June 2010
- ✓ Sharma V., Part B- An Overview of cyber law, paper I, Introduction to the cyber world and cyber Law published on http://www.elearningilidelhi.org/eSikshak/other/Courses/Course101/Module9/ over view of cyber law
- ✓ Tripathy, P., Walini “Emerging scenario of Indian Banking Industry” Mahamaya Publishing House, New Delhi 2005.