Volume : 5 | Issue : 4 | April 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

Research Paper

Electronic Crime in Indian Banking Sector

Law

KEYWORDS : ATM, electronic crime and cyber crime.

Dr. Prativa Panda | Reader, University law College, Utkal University, Bhubaneswar-4

ABSTRACT

In the present globalizes scenario, information technology is the most important and controversial term. It is the most powerful technology which is fast, quick and accurate in all sectors. Increased use of information and communication technology (ICT) such as computers, mobile phones, Internet, and other associated technologies are the routes which gave emergence to lot of constructive work as well as destructive work. The destructive activities are considered as "electronic crime" which includes spamming, credit card fraud, ATM frauds, Money laundering, Phishing, Identity theft, denial of service and other host contributing crime in the Indian Banking sector. This paper has made an attempt to analyze the impact of electronic crime in Indian banking sector.

INTRODUCTION:

Computers and Internet are also the new powerful information tools in present era, these new technologies brings out new threats opportunities such as denial of service attacks, viruses, unauthorized entry, information tampering, cyber stalking, spamming, paper-jacking, dumping or phone-napping and computer damage[1]. **Evolution of Electronic Crime:**

Electronic crime started during the period of 1960" s in the form of "Hacking". In the period of 1970's presence of computer introduced new crimes as computer crimes in the form of privacy violation, phone tapping, trespassing and distribution of illicit materials. Then, later in the period of 1980's electronic systems crime emerges in the form of software piracy, copyright violations and introduction of viruses. The extent of damage after 1980's increased due to the highly sophisticated electronic systems. These electronic crimes gave a wider impact on the Indian market, international market, Banking sector and other areas also. Therefore, presently electronic crime became a major subject of concern worldwide[2]

Electronic Crime:

Computers, Internet and other electronic medium are the commanding information tools to make possible immediate exchange and distribution of data, images and materials. Information Technology brings growth and development and its fraudulent practices are bitterly termed as cyber-crime or computer crime, e-crime, hi-tech crime or Electronic crime.

Computer and Internet are the powerful in a row tools including financial networks, communication systems, power stations, modern automobiles and appliances. Quite a few innovative technologies are also extensively available which are responsible for causing electronic crime. They are denial of service attacks, viruses, unauthorized entry, information tampering, cyber stalking, spamming, paper-jacking, dumping or phone-napping and computer damage.[3]

The internet services and web technologies in India is growing at a fast level. These technologies have it own pros and cons. The pros are the benefits and advantages but the cons are named as "CYBER CRIME" or "Electronic Crime". These crimes take place due to certain loop-holes which result in e-mail espionage, credit card fraud, spams, software piracy etc.[4]

Features of Electronic Crime:

Electronic crime has its some attractive features such as

1. Anonymity
2. Global reach to a numerous places such as issues of jurisdiction, disparate criminal laws and the potential for large scale victimization
3. Speed of crimes
4. Electronic crime potential for deliberate exploitation of issues and differences
5. Volatility and transact nature

Electronic Crime in Banking Sector:

Banking system is the lifeblood and backbone of the economy. Information Technology has become the backbone of the banking system. It provides a tremendous support to the ever –increasing challenges and banking requirements. Presently, banks cannot think of introducing financial product without the presence of Information Technology[5].

The Indian Banking sector is riding up with numerous revolutionary changes to transform the "Brick-and-mortar" bank branches to a modified network system in "core banking solutions". The banking sector consists of public sector, private sector and foreign banks. With this a number of IT based banking products services and solutions are available[6].The most common IT based products available are

1. Phone Banking
2. ATM facility
3. Credit, Debit and Smart cards
4. Internet banking
5. Mobile Banking
6. SWIFT Network
7. INFINET Network etc

Computer device used as a medium of target to commit crime - Electronic crime is used as a target to commit crime It includes

- Sabotage of computer systems or computer networks
- Sabotage of operating systems and programmes
- Theft of data/ information
- Theft of intellectual property such as computer software

Computer is working as an instrument of the crime. Banking criminals are using various electronic medium such as internet, e-mail, and flash encrypted messages etc to commit crime. This crime through computer network takes place in the banking sector. They are

- Fraudulent use of Automated Teller Machine (ATMs) cards and accounts
- Credit card frauds
- Frauds involving electronic funds transfers (EFTs)
- Telecommunication frauds
- Frauds relating to E-commerce and EDI

TYPES OF ELECTRONIC CRIME IN INDIAN BANKING SECTOR:

1 ***Credit card Fraud***- A major kind of electronic crime is "credit card fraud". Indian banking sector is introducing new innovations against counterfeiting and fraud, which are highly sophisticated to profiting from or beating these systems. Most of the credit card fraud is committed with the use of counterfeited

Volume : 5 | Issue : 4 | April 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

cards. Credit card fraud is also termed as "Identity Theft" in which a person may use the identity of other person for exercising fraud or deception.[7] Credit card fraud in banking sector can be committed as

- Use of unauthorized account or personal information to consider as an act of criminal deception
- Illegal or unauthorized use of account for personal gain
- Misrepresentation of account information to obtain services

Several new security measures are introduced to gradually to reduce the credit card fraud in one part but it swiftly shifts to other part. Therefore, the problem of credit card fraud is serious and occurring by stealing the cards and the accompanying information at the time of transaction.

2 ***Money Laundering:*** Throughout the precedent two decades, IT and Internet technologies have reached each one nook and corner of the world. E-commerce has come into existence due to the attributes of Internet like ease of use, speed, anonymity and its International nature. Internet has transformed the planet into a frontier excluding market place that never sleeps. Computer networks and Internet authorize relocate of funds electronically between trading partners, businesses and consumers. This shift can be done in many ways like use of credit cards, Internet banking, e-cash, e- wallet etc. for example, smart cards. In some other forms of computer-based e-money, there is no upper limit.

Two persons also can shift funds in a straight line using e- wallets. This problem is further compounded by the fact that, in several countries, non-financial institutions are also allowed to issue e-money. Monitoring the behavior of these institutions in a habitual manner is not possible. Earlier, cross-border transactions were controlled by the central banks of respective countries. With the entrance of Internet commerce, the jurisdictional technicalities come into battle and it is another area that is being exploited by the money launderers. The competence to transfer limitless amounts of money without having to go through strict checks makes cyber money laundering an attractive proposition.

The main objective of these guidelines is to prevent the banking transactions from being used by criminal intentionally or unintentionally as an element of money laundering. Banks and financial institutions are the core targets or focus on anti-money laundering practices and combating of financial terrorism laws due to their vulnerability and adherence of these laws to combat money laundering a counter financing.[8] The money laundering reduces the officially authorized quantity of the banks business causes fluctuations in the exchange rate. Money laundering can undermine the credibility of the banking system. Facilitating the activities of launderers even inadvertently can set in motion the banks into problems with law enforcement agencies and also governments.

3 ***ATMs Frauds:*** Over the past three decades, large number of banking customers depends on the ATM to conveniently meeting their banking needs. In the recent years, there have been a large number of accidents of ATMs frauds. It is necessary to manage the risk associated with ATM fraud as well as diminishing its impact on the important issues that face financial institutions as fraud techniques to become more advanced with increased occurrences. The prevailing contemporary era has replaced long-established monetary instruments from a paper and metal based currency to "plastic money" in the form of credit cards, debit cards, etc. This has resulted in the escalating utilize of ATM all over the world. The use of ATM is not only safe and sound but also suitable. This safety and convenience, has an evil side which is reflected in the form of "ATM FRAUDS" that is an international problem. The use of plastic money is increasing for payment of shopping bills, electricity bills, school fees, phone bills, insurance premium, travelling bills and even petrol bills.

CONCLUSION: At last it can be concluded that to eliminate cyber crime from the cyber space is not a possible task but it is possible to have a regular check on banking activities and transactions. The only promising step is to create awareness among people about their rights and duties and further making the application of the laws more stringent to check crime. There is a need to bring changes in the Information Technology Act to make it more effective to combat electronic crime in banking sector.

END NOTES:

1 Jain .A (2005*). "Cyber Crime: Issues & Threats and management"* 2nd Volume, Printed at Chawla offset Press, Delhi, p.1

2 Olufunke.O.O, (2010). *"Computer Crimes and Counter Measures in the Nigerian Banking Sector"* , Journal of Internet Banking and Commerce, April, Volume 15, Issue no.1, p.2

3 Jain.A, 2005

4 www.scribd.com

5 (Reddy.G.N, 2009).

6 BhasinM (2007). *"Mitigating Cyber Threats to Banking Industry"* , The Chartered Accountant, April 2007, p.1622-1623 (Sharma.A.K & Nanda.G.L, 2006)- Batra.H.K (2009). *"Money Laundering Challenges Before Banks"* ,Chartered Financial Analyst, November,p.65

7 Sharma.A.K & Nanda.G.L (2006). *" Frauds in Credit Card Business"* , Banking Finance, July , Volume , Issue no.7, p.15

8 Batra.H.K (2009). *"Money Laundering Challenges Before Banks"* ,Chartered Financial Analyst, November,p.65

REFERENCE:

1. Ahuja.A.V (2010).*"Cyber Crime in Banking Sector"* available at http://www.scribd.com/doc/28079943/Cyber-Crime-in-Banking-sector, p.6