Advances in Economics and Business Management (AEBM)
p-ISSN: 2394-1545; e-ISSN: 2394-1553; Volume 4, Issue 4; April-June, 2017, pp. 204-208

http://www.krishisanskriti.org/Publication.html

Digitalization of Money Transactions and Threats to Consumers in e-Banking Regime

Gagandeep Kaur

University of Petroleum and Energy Studies Dehradun
E-mail: gdkaur17@gmail.com

Abstract—*Digitalization is the integration of digital technologies into everyday life of almost everything under the sun by the revolution of Information and Communication Technology. In the last decade with the rise of e-Commerce new web-based companies have set up providing online services. One of the most important transformations is the digitalization of money transactions through e-Banking services. E-Banking is a valuable medium and a crucial piece of infrastructure which has drastically modified economic sectors. Digitalization, Computer software, Hardware, Internet Technology and presently 4G has created novice opportunities of communication, e-Commerce transactions, money transfer and e-Banking transactions. However, E-banking transactions are vulnerable to Cyber Attacks against confidential sensitive information. Among all the Cyber Attacks Phishing and Pharming are major threats. Phishing and Pharming is a deceptive attempt that targets an individual or an organization. It seeks unauthorized access to confidential data or personal credentials such as credit card information, password, CVV number, address, name and date of birth etc. by an email address that poses as a reputable person or organization. It has become a major threat in e-Commercial transactions. If these threats cannot be ceased, people cannot trust online transactions that include authentication over credentials. In this article the basic emphasis is: (a) generally on the e-Banking frauds and particularly on the Phishing and Pharming; and (b) Analysis of legal control mechanism to answer these emerging cyber threats in e-money transactions.*

Keywords*: E-Banking, Phishing, Pharming, IT Act, 2000.*

1. INTRODUCTION

Wonderful and unimagined advancements in Internet and Communication Technology have revolutionized today's landscape of commercial transactions. Now a day, technological advancements have brought the entire cosmos to a situation where everything is moving at a great pace.[i] Over the last two decades the global arena has witnessed as well experienced a tremendous growth in the field of Information Technology wherein entire world has turned from postal to portal world.[ii] In the web world no business or commerce can afford to remain on the sidelines as a result e-Commerce has become an integral part of 21st century.[iii]

e- Commerce is an economic solvent. It dissolves old business models, changes the cost structures, and re-arranges links among buyers, sellers and everyone in between. It will not incorrect to state that e-Commerce is a chemical that reacts with everything it touches.[iv] e-Commerce is to the information revolution what the railroad was to the industrial revolution- And like the rail road; e-commerce has created a new and charismatic boom by rapidly changing the economy, society and every segment of society.

One of the most outstanding developments in e-commercial transaction has been the geometric expansion of 'On-line Banking' or 'e-Banking. Online banking or e-Banking has made inroads in the lives of every walk of human life and the entire business world is surrounded by the benefits bestowed by 'e-Banking'.[v] E-Money appears to be the latest payment vehicle. e- Banking implies provisions of banking services through electronic delivery channels. In India electronic banking has been around for quite some time in the form of automatic teller machines (ATMs) and telephone transactions. With the Internet - a new delivery channel that has facilitated banking transactions for both customers and banks. Electronic banking involves many different types of transactions namely:[vi] Electronic Fund Transfer (EFT), Direct Deposits, Pay by Phone Systems, Personal Computer Banking, Debit Card Purchase, E- Money and Electronic Check Conversion.

2. NATURE OF FRAUDS IN ONLINE PAYMENT MECHANISM OF E-COMMERCE

Since times immemorial fraudulent activities have been deeply embedded in business. In Indian physical banking industry, the classification of banking frauds used to be like: misappropriation, criminal breach of trust, fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts, conversion of property, unauthorized credit facilities extended for reward or for illegal gratification, negligence, cash shortages, cheating, forgery and irregularities in foreign exchange transactions etc., etc.[vii] Till today frauds are committed on consumers in markets, however, modes of cheatings have become very refined and sophisticated. On one hand, technological advancements have provided a bundle of facilities to the

consumers in cyber world, however, on the other hand, novice modes of committing frauds have also come into existence which is very difficult to recognize and investigate. Frauds like brand spoofing, phishing, identify theft and other online frauds continue to be a major issue of retail banking and banks all over the world. The following types of frauds are generally committed in e- Money transactions:

2.1 Cyber Money Laundering or e-Money Laundering

2.2 Skimming

2.3 Phishing

2.4 Pharming

2.1 Cyber Money Laundering or e-Money Laundering

The term 'money laundering' was used in legal context for the first time in the *Watergate Scandal case* of United States in 1973 and it meant, "a progress of converting money derived from illegal activities into a legally consumable form." Money laundering is a cybercrime in which money is illegally downloaded while it is in transmit.[viii] Hawala is a special kind of underground banking system, which is considered highly efficient means to launder money. e- Money laundering is not a single act but it is derivative crime which involves three basic steps, namely, (i) Placement (ii) Layering and (iii) Integration. It means "placement" of the dirty money into the financial system; "layering", where the dirty money that is present in the banking or financial system, is moved through the global financial system to hide its origins or separate it from its illegal source, and "integration" where the illicit funds are blended back into the economy and become indistinguishable from legitimate funds.[ix] Money laundering is one of the most common financial activities connected to illicit financial schemes, tax evasion, narcotics, corporate frauds, government corruption and white collar crimes.[x]

2.2 Skimming

CVV (Customer verification value) means Card Verification Value (CVV) is a combination of features used in credit, debit and automated teller machine (ATM) cards for the purpose of establishing the owner's identity and minimizing the risk of fraud. The CVV is also known as the card verification code (CVC) or card security code (CSC).[xi] Skimming is the fraudster's answer to the CVV (Customer Verification Value) introduced by the issuers. CVV is an algorithm (a code) which is very difficult to break through. The fraudster, therefore, does not bother to do so. He/she (fraudster) simply colludes with a merchant or merchants. He/she then provides the merchant with a terminal similar to the one provided to the merchant by the bank. The difference being that the fraudster's terminal is capable of actually recording the data on each magastripe which is swiped through the terminal while the banks terminal only processes the data but does not have a recording facility. The merchant swipes the card twice; once on the bank's terminal and again on the fraudster's terminal. The CVV which is encoded on the magastripe and is decoded on the terminal gets recorded on the fraudster's terminal. The fraudster has now genuine card information along with the CVV for each card. This is a goldmine for making counterfeit cards as far as the fraudster is concerned.[xii]

2.3 Phishing

A phishing expedition, like the 'fishing' expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Phishing is an e-mail scam where the fraudster leads the card-holder to believe that he is responding to a legitimate e-mail request from a known or well-known organization.[xiii] Phishing is a deceptive online attempt by a third party to obtain confidential information for financial gain.

Phishing on Internet is a form of 'Passing Off'. Phishing is a form of Internet fraud by using passing off tactics where a person pretends to be legitimate association such as s a bank or an insurance company in order to extract personal data from a customer such as his access codes, password, account number, address, mobile number and residence proof etc., etc. The personal data so collected by misrepresenting the identity of the legitimate party is generally used for siphoning out money from the victim's account. In this type of fraud the messages appear to come from well-known and trustworthy web sites. Web sites that are popularly and frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online.

2.4 Pharming or Spoofing

Hackers who attempt to hide their true identity often spoof or misrepresent themselves by making fake web addresses and web pages as someone else. Spoofing a web site is also called "pharming", which involves redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination. Links that are designed to lead to one site can be reset to send users to a totally unrelated site-one that benefits the hacker. The word "spoof" means to hoax, trick, or deceive. Therefore, in the IT world, spoofing means tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

Spoofing can take place on the Internet in several different ways, namely, (i) E-mail Spoofing[xiv]; (ii) IP Spoofing and (iii) Spoofing can be done by simply faking an identity[xv]. Although spoofing does not directly damage files or network servers, it threatens the integrity of a web site. If hackers redirect customers to a fake web site that looks almost exactly like the true site they can then collect and process orders from the web site. Or, if the intent is to disrupt rather than steal, hackers can alter orders, or change products order and then send them to the true site for processing and delivery. Customers become dissatisfied with the improper order shipment and the company may have huge inventory

fluctuations that impact its operations. Junk or spam web sites typically appear on search results, and do not involve e-mail. These sites cloak their identities by using domain names similar to legitimate firm names, post their names on open web forums, and redirect traffic to known spammer-redirection domains such as vip -online search, info searchadv. com and web resources. info.[xvi]

3. TREND OF INDIAN JUDICIARY ON E-BANKING CRIMES: AN OVERVIEW

One of the important cases was ***National Association of Software and Services Companies v. Ajay Sood***[xvii] - This was a reasoned order approving a settlement agreement between the plaintiff and the defendants in a case which dealt with the issue of 'phishing', wherein a decree of 16 lakhs was passed in favor of the plaintiffs. The suit was filed for a decree of permanent injunction restraining the defendants or any person acting under their authority from circulating fraudulent e-mails; that were purportedly originating from the plaintiff of using the trade mark 'NASSCOM'. The court held that it would criminalize the act of creating a phishing website regardless of whether any visitors to the website suffered any actual damages. This decision of High Court of Delhi is considered as a landmark decision in the history of Indian cybercrimes. The court has made phishing as punishable cyber offence although there is no specific statutory legislation to this effect; and expressed a view that phishing has developed as a sophisticated method of committing organized cybercrime by befooling even the most experienced and knowledgeable persons.

ICICI Bank Phishing case. E-mails, that is considered as the most convenient form of communication can bring some shocking surprises. Few ICICI Bank customers in Mumbai received an e-mail from someone who posed as an official of the bank and asked for sensitive information like Internet login name and password of the account holder and directed them to a web page which resembled with the official site page of the bank. The e-mail seemed so genuine that some users even clicked on the URL given in the mail to a Web page that resembled the official site. When some customers wrote and asked to find out the purpose of the e-mail, the bank officials were left with no option except to register a complaint with the police. Such a scam is known as 'phishing.' It is actually a banking scam and a warning against which had been issued by many International banks.[xviii]

The notorious ***World Wide Nigerian Scam***[xix] deserves a special mention. This scam is better known as Advance Fee Fund (AFF) or Nigerian Fraud or the '419 Fraud'. This scam is committed as follows: The victim (target) receives and unsolicited fax, e-mail or letter concerning Nigeria or any other African nation, mostly from West Africa such as Ghana, Togo, Liberia, Sierra, Leone, Ivory Coast etc; requesting for legal and legitimate business proposal or service contracts. The victim is asked to pay on advance fee of some kind which may be in the form of 'transfer tax', 'performance bond' or for credit privileges. Once the victim pays the fee, many more requests for advance payments on one pretext or another come to the victim until he either decides to quit or runs out of money, or both.[xx] The moment victim gives his/ her account details, he/she has to suffer a huge amount of financial loss. Alarmed by the widespread *Nigerian '419 Fraud'* the Government of USA, UK, Canada, South Africa etc., etc. have warned the business community to be alert and not to respond to 419 letters, instead file a complaint against the sender with the national law enforcement agency as also to Nigerian Embassy and the Central Bank of Nigeria.

It has been observed that Indian judiciary is taking strong steps against newly emerged e- Banking frauds. These decisions of the hon'ble courts provide a sound ground for the growth of stringent provisions in cyber law against online financial frauds. However, it is need of the time to make some amendments in the Information Technology Act, 2000 (2008) and add penal provisions for the offences against consumers during e- Banking transactions. The following pages depict the legal control mechanism to combat frauds in e- banking from which it is crystal clear that in Indian cyber jurisprudence, it is very important to enact strict penal as well as compensatory provisions.

4. LEGAL CONTROL MECHANISM TO COMBAT FRAUDS IN E-BANKING IN INDIA

With the advent of Information Technology interest in the right of privacy has increased in the 1960s and 1970s. The genesis of modern legislation in the area of data privacy can be traced to the first data protection law in the world enacted in Germany in 1970. This was followed by National laws in Sweden (1973), the United States (1974) and in France (1978). Two crucial International instruments evolved from these laws i.e. the Council of Europe's 1981 Convention for the protection of individuals with regard to the Automatic Processing of Personal Data; and the Organization for Economic Cooperation and Development's (OECD) guidelines governing the Protection of Privacy and Trans Border Data.

Several countries have taken their data protection laws from these two documents. In India in the case of *Shankarlal Agarwalla v. State Bank of India*[xxi] banks are required to maintain secrecy of the accounts of their customer's. The exceptions to the rule are as under: (a) where the disclosure was under compulsion by law, (b) where there was a duty to the public to disclose, (c) where the interest of the bank requires disclosure and (d) where the disclosure was made by express or implied consent of the customer.[xxii]

In India e- banking legislations are: The Negotiable Instruments Act, 1881, The Prevention of Money Laundering Act, 2002 (PMLA) & Prevention of Money Laundering Rules (PMLR), The Payment and Settlement Systems Act, 2007

(PSS Act), The Information Technology Act, 2000 and The Information Technology (Amendment) Act, 2008.

The *Information Technology (Amendment) Act 2008* has made specific provisions dealing with: (a) Protection of sensitive personal data: security practices and procedures that must be followed by organisations dealing with sensitive personal data (Data Privacy Rules) 2011,

(b) Due diligence to be observed by intermediaries, and

(c) Guidelines for cybercafés.

Under the *Information Technology (Amendment) Act 2008* some of data protection provisions are as follows: Under Section 43-A[xxiii], a body corporate that possesses, deals or handles sensitive data in a computer resource is liable to pay compensation if it is negligent in implementing and maintaining reasonable security practices and procedures, and such negligence results in wrongful loss or wrongful gain to any person. Under section 66 if any person does any act referred to in section 43[xxiv], with dishonest and fraudulent intention, he shall be punished with the imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. In this context Section 72[xxv] and 72-A[xxvi] of the amended IT Act, 2000 are also of relevance. Section 72 of the Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any electronic record, book, register, correspondence, information, document or any other material etc., etc. and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment up to two years or with fine upt o one lakh or with both. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. Under section 72 A offenders shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

5. CONCLUSION

Technology... is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other.

C.P. Snow

In the light of above mentioned statement it seems to be very true that on the one hand, e- banking has provided quick, easy and convenient services available 24 hours, however, on the other hand, it has provided a fertile ground for fraudulent activities. Mostly, victims of these crimes are innocent people who avail the services of novice high-tech network technology without awareness of dragon of cyber offenses. In India, whenever any illegal act occurs in cyberspace, all eyes look upon the Information Technology Act, 2000 (2008) for solution. After analysis of provisions under this Act, it is seen that most of the provisions are focused on disclosing of personal information either by body corporate or otherwise and their punishment has been described. No mandatory protection has been provided to consumers against offences like Phishing, Pharming, Cyber Money Laundering, ATM Frauds and other financial frauds wherein innocent consumers are cheated and defrauded. The Information Technology Act, 2000 (2008) has covered fraudulent financial activities indirectly. The lack of a comprehensive legislation pertaining to privacy and data protection has been a matter of great concern in India. With the strict regulations and privacy norms mandated by the Reserve Bank of India, the Indian financial industry has started the process of sensitizing the Government. RBI has issued guidelines for the innocent public because the tools of committing bank frauds have become highly sophisticated. An ordinary individual is not able to recognize that he/she has become victim of online frauds. It has been suggested that in order to provide strong shield to consumers from online financial frauds, India needs specific stringent and clear legislation.

REFERENCES

i N. Subramanian, *Introduction to Computers: Fundamentals of Computer Science*, Tata McGraw Hill Publishing Company Limited, New Delhi, 1999, p. 8.

ii Peeyush Kumar Pandey and Sunil Kumar Pandey, "Information Technology and E-Commerce" in S.B. Verma (edited), *Information Technology and Management*, Deep and Deep Publications Pvt. Ltd., New Delhi, 2005, pp. 145-147.

iii V.P. Gulati, "Information Management: Issues and Challenges" in S.B. Verma (edited), *Information Technology and Management*, Deep and Deep Publications Pvt. Ltd., New Delhi, 2005, p. 289.

iv Ravi Kolakata and Marica Robinson, *e-Business 2.0: Roadmap for Success*, Anubha Printers, Pearson, New Delhi, 2009, p. 28.

v Ravi Kolakata and Marica Robinson, *e-Business 2.0: Roadmap for Success*, Anubha Printers, Pearson, New Delhi, 2009, p. 28.

vi "Electronic Banking", FTC Facts for Consumer, Focus on Credit, Federal Trade Commission for the Consumer, March, 2012, Bureau of Consumer Protection, Division of Consumer and Business Education, Retrieved from http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre14.pdf.

vii Retrieved from:< http://rbidocs.rbi.org.in/rdocs/notification/PDFs/80CR010712FL.pdf>.

viii James R. Richards, *Transnational Criminal Organizations: Cyber Crime & Money Laundering*, CRC Press, New York, 1999, p. 44.

ix ibid., p. 45.

x Lech J. Janczewski, Andrew Michael Colarik, *Cyber Warfare and Cyber Terrorism*, Idea Group Inc. (IGI), Information Science Reference, New York, 2008, p. 143.

xi Retrieved from:<http://searchfinancialsecurity.techtarget.com/definition/card-verification-value>, visited on 15 December, 2014.

xii Retrieved from:< http://searchfinancialsecurity.techtarget.com/definition/card-verification-value.

[xiii] Retrieved from: http://searchsecurity.techtarget.com/definition/phishing.

[xiv] e-mail Spoofing: e-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Fortunately, most e-mail servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP, which allows them to use fake e-mail addresses. Therefore, it is possible to receive e-mail from an address that is not the actual address of the person sending the message. Retrieved from : < http://www.techterms.com/definition/spoofing>.

[xv] For example, when posting on Web discussion board, a user may pretend he is the representative for a certain company, when he/she actually has no association with the organization. In online chat rooms, users may fake their age, gender, and location.

[xvi] Kenneth C. Laudon and Caral Guercio Traver, *E-Commerce : Business, Technology and Society*, Pearson Education, Delhi, 2008, p. 276.

[xvii] 119(2005) DLT 596, 2005(30) PTC 437(Del).

[xviii] ICICI Bank phishing scam targets customers in India, Retrieved from: <http://www.net- security.org/secworld.php?id=4051.

[xix] Retrieved from:< http://www.fbi.gov/scams-safety/fraud/fraud#419>.

[xx] Vishwanath Paranjape, 2010, p. 140.

[xxi] Shankarlal Agarwalla v. State Bank of India and Anr. AIR 1987 Cal 29.

[xxii] Retrieved from :<http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage&ID=624>.

[xxiii] Section 43 A of the Information Technology (Amendment) Act, 2008: Compensation for failure to protect data (Inserted vide ITAA 2006).

[xxiv] Section 43 of the Information Technology Act 2000 provides penalty and compensation for damage to computer, computer system, computer network, computer data base and many other computer related offences.

[xxv] Section 72 of the Information Technology Act 2000: Penalty for breach of confidentiality and privacy.

[xxvi] Section 72-A of the Information Technology (Amendment) Act 2008: Punishment for Disclosure of information in breach of lawful contract: (Inserted vide ITAA-2008).