Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.10, 2015

An Appraisal of Cyber Laws with Reference to E-Banking in Pakistan

Rameez Anjum
Department of Law, Government College University, Faisalabad, Pakistan

Ms. Fozia Naseem (Supervisor)
Lecturer at Department of Law, Government College University, Faisalabad, Pakistan

Abstract
The Information and Communication Technology (ICT) has revolutionized almost every aspect of human endeavor. Increased use of ICT such as computers, cellular phones, internet and other associated technologies are the routes which gave emergence to a lot of constructive as well as destructive work. The constructive work includes simplicity in business transactions provided convenient, effective, speedy and smooth processes. The destructive activities are considered as "electronic or cyber crimes" such as Identity theft, credit card and ATM frauds, criminal activities, spamming, phishing and other web-based crimes. This study will identify the adverse effects of the cyber crimes on e-retailing, effects of cyber crimes on financial transactions in e-banking sector, the present need to formulate policy framework, national legislation and independent investigation authority to penalize such criminals.
Keywords: ATM, E-Banking, E-Commerce, EFT, E-Payment, ICT, M-Banking, PECO

1. INTRODUCTION

Technology has undergone tremendous changes with the passage of time. Innovation in technology is an on-going process. Information Technology (IT) is the automatic system generated process, production and control mechanism used via computer, web and wireless based telecommunication. Today a number of variations have occurred in every sphere of life and Business has also faced many changes, the most remarkable of which is technology which has not only created new products but a constant opportunity to services market. It has succeeded in developing a system oriented business with a much better and reliable management processes. Electronic business or it may be called e-commerce in the present era referred to the use of such electronic devices and technologies in conducting the business either between a business and a customer or simply between two parties.

With this innovation in banking sectors, individuals can make their account enquiries and transfer funds speedily without any need to go to the bank hall. We have now gradually moved towards a cashless society where consumers no longer have to carry hard cash for their purchases. For example, a bank customer can subscribe to public offers made by companies or buy airline tickets (e-ticket) by transferring the money directly from their accounts, or purchase different goods and acquire services by electronic transfer of credit to the sellers' account. Broadly speaking, this payment system can be coined as e-payment. Banks have also introduced mobile banking services termed as "m-banking" as majority of people now own mobile phones to cater the need of such customers who are always on the move. "Mobile banking" channel facilitates the individuals to check their account balances and transfer funds while using their cell phones.

The delivery channels today in electronic Banking are quite numerous i.e., Automatic Teller Machine (ATM), Point of Sales (POS), Visa Cards, Telephone Banking, Online Banking etc. Internet is increasingly used by banks as a medium of tendering the services and products to the numerous customers. Almost all the banks have a web-based structure; this type of Banking is referred to as Internet Banking which is virtually a part of "Electronic Banking".

The Government of Pakistan has boosted electronic banking with the announcement and promulgation of the Electronic Transaction Ordinance 2002. The digital signatures and documentation system supported by a legal spectrum was provided which helped in reducing the risks linked with the use of electronic media in business. Presently, almost all the banks in Pakistan have setup their own ATM networks, banks now issue credit and debit cards to their customers and have also linked with one or two operating ATM Switch Networks referred to as "1-Link" or "M-net" networks.

2. RESEARCH QUESTION

What are the proposed threats caused to e-banking sector, their unintended consequences and the present need to formulate policy framework, domestic legislation and the establishment of an independent agency for the investigation, control and penalizing the cyber criminals?

3. REVIEW OF LITERATURE

Banking is one of such most significant business sectors and is an ideal ground where this successfully developed

E-commerce could flourish. (Kardaras and Papathanassiou, 2001)

Harold and Jeff argue that Financial Sector will have to alter their traditional operating practices to remain viable in the 1990s and the decades that follow. They claim that the most significant shortcoming in the banking industry today is a wide spread failure on the part of senior management in banks to grasp the importance of technology and incorporate it into their strategic plans accordingly. (Harold and Jeff, 1995)

Woherem (2000) claimed that only banks have overhauled the whole of their payment and delivery systems and apply ICT to their operations are likely to survive and prosper in the new millennium. He advices banks to re-examine their service and delivery systems in order to properly position them within the framework of the dictates of the dynamism of information and communication technology. The banking industry has witnessed tremendous changes linked with the developments in ICT over the years.

Information Technology has brought these few innovations which have resulted in changing the entire dynamics of banking as much as the e-banking revolution. All over the world, banks are restructuring and reorganizing their business strategies to adamant to such new business opportunities offered by e-banking. Electronic banking was believed to have started in the early 1980s. Advancement in Information Technology has played a vital role not only in improving delivery standards but also helped in providing time constraint services in the Banking industry. In the simplest term, Automated Teller Machines (ATM) and deposit machines can now facilitate customers to carry out banking transactions even after banking hours.

Commercial Banks in Pakistani provide the following online services and products. (1) Inquiries include Account balance inquiry, Account statement inquiry, Cheque inquiry and Fixed deposit inquiry (2) Payments which include Credit card payments, Transfer of funds, Direct payments or remittance, Utility bills payments (3) Requests including Cheque-book issuing requests, marking Stop payment requests, Demand draft requests and fixed deposit requests (4) Downloads comprising of Customers' profile, Statement download and any other guideline or information download. (Akhtar, 2008)

However, after the emergence of Information and Communication Technology, the security issue has become a chief concern in the Banking Industry today, as banking is based highly on trust from its customers. While a number of risks and threats have also emerged due to lapse in the technology. They include the risk of hackers, technological failure, denial of service attacks, breach of privacy of customers' information and opportunities for hackers to commit fraud, all of this happened due to the anonymity and identity theft issues occurred in electronic transactions. Not only the security lapses and flaws can cause serious damage to public confidence but lacking of due diligence and countermeasures might raise a serious threat to the stability of a financial institution or collapse the whole of banking system. Hence, it has become quite necessary to introduce the comprehensive security measures and appropriate security concerns should be made at ease so that the banking industry could be able to attract those consumers who were previously not interested in using e-banking. Further, the banks should also improve their security polices so that financial transaction losses could be avoided and tackled without causing any damage to the brand of the bank.

4. MATERIALS AND METHODS

The potential to control e-risk in the business and financial sector is a prime concern as the developments in banking, industrial, economic and regulatory conditions have created bigger challenges for businesses. Cyberspace is open to villains who are always on the move to exploit computer networks. Hackers try to hack into a firm's computer system to fulfill their financial needs. If access is gained to a system, there is every possibility to achieve their goals as well as causing much damage to a system by erasing, encrypting, modifying and deleting data.

The study presents those types of cyber crimes which directly or indirectly influence the economy of a nation or exploit the financial systems without border constraints. As the computer, mobile and internet technologies have advanced, criminals have found means to achieve their old-fashioned goals such as fraud, theft, harassment, denial of service attacks and intimidation. Crimes committed in the cyberspace by the criminals are known as cyber crimes such as Phishing, Spamming, Spoofing, Cyber Terrorism, Cyber Stalking, Electronic Spam Emails and especially electronic banking crimes committed in cyber space such as ATM frauds, electronic payment frauds, transactional payment frauds, stealing of information, hacking of bank accounts, credit and debits cards frauds etc.

Phishing in its simplest form defined as a high-tech identity theft which not only helps the criminals to steal personal identity and information, but an act of fraud also against the financial institutions and legitimate businesses. It is a type of bullying or electronic identity theft in which website spoofing and social engineering techniques are used to trap a user and extort to reveal his or her confidential information having economic value which later is employed by miscreants who aim to earn an easy profit by illegal financial transactions means. A few laws have been made on the subject:

- Anti-Phishing Act of 2005 [In USA]
- Fraud Act, 2006 [in UK]
- Anti-Spam Legislation in Canada.

Cyber terrorism includes almost all the possible attacks against technological infrastructures which would try to dismantle the banks, international financial transactions, insurances and the stock exchanges. If such attacks are committed on a larger scale, there is every possibility that the people around the globe will lose trust and confidence in the economic system, ended in unprecedented financial losses and probably collapsing the world's economic position. A few countries have legislated to protect their sovereignties from these kind of attacks which are:

- Cyber Security Act of 2012
- Cyber Intelligence Sharing and Protection Act.
- National Cyber Security Policy of India 2013
- Information Technology Act, 2000

In web-based services, e-mail is an earliest and excellent communication device which is frequently used by the companies to introduce new products and services. However, at the same time, it is also used frequently in delivering unwanted material such as malicious contents – causing significant damage to computers and individuals. Spam email generally includes the delivery of scams. Scams are projected to disclose information, while identity theft and fraudulent activities are the ultimate outcome of such disclosure. Spam email is commonly known as junk email or is also termed as "unsolicited bulk email" (*UBE*). The potential victims are forced or coerced to provide their confidential information such as credit card details, system IDs or bank account information. Finally, victims who are trapped in such baits discover that thousands to millions of dollars have been stolen from their bank accounts. CAN-SPAM Act of 2003, promulgated in USA is remarkable in this regard.

The term 'Cyber stalking' involves the use of information technology especially Internet, by an individual or a group of persons to intimidate, harass and cause fear. Common abusive behaviours that occur with the use of technology include monitoring communications with others, transmitting threats, making false accusations, damaging to confidential equipment or data, stealing identity, soliciting minors for sexual abuse or some other types of assault. Following enactments are important to shun the criminals from performing such crimes which are noted as:

- Stalking Amendment Act (1999) in Australia
- Electronic Communications Act, 2001.
- US Federal Anti-Cyber-Stalking law

But unfortunately, banking sector especially electronic banking (e-banking) has become more susceptible to such threats or risks posed by these innovations. These threats or risks are posing great damage because there is a juridical backlog, lack of training on the subject to investigate the electronic crimes. The cases of online frauds, transactional payment frauds and account hack-overs have become very common today.

5. RESULTS AND DISCUSSION

The use of electronic banking increases the necessity for regulation arises. Accordingly certain standards for regulation have also been defined. They are categorized as:

1. Technology and Security Standards
2. Legal Issues

As regards Technology issues, the security for transactions conducted on the Net is the main issue. The measures to be adopted by banks are all centered around this point. Some of the measures that Banks have adopted in regulation of E-Banking are:

a. Mandatory licensing and approval by State Bank of Pakistan for Banks for providing Internet Banking facilities.
b. Bilateral agreements between customers and banks for e-banking, underlining the rights and liabilities of each other.
c. E-banking products must be offered to the account holders only and not in other jurisdictions.
d. The services must be offered in local currency alone and not otherwise.
e. Failure or Breach of Security systems to be reported to SBP for audit and inspection.
f. SBP Regulations for Banks made applicable to Internet Banking also.
g. Outsourcing guidelines by Banks to third parties for effective risk management.
h. For settling of transactions only 'Inter Bank Payment Gateways' must be used, with real time settlements.

As far as the legal frame work is concerned, Pakistan is falling behind in this respect. Generally, Pakistan is relying on those laws which were made almost a century ago. Technologies are moving at a great pace today and we are much aware of the concepts of global trade, internet banking or electronic commerce. However, if Pakistan is to become viable with this ever-changing environment, then it must replace the traditional laws to adjust to the atmosphere. The present structure especially electronic banking needs a strong Legal Infrastructure to protect e-banking framework from all of its vulnerabilities otherwise the banking structure would be a total collapse resulting in total economic massacre.

Feeling the impulse, the former President of Pakistan named as Pervaiz Musharraf implemented

Electronic Transactions Ordinance (ECO) 2002. It was the first initiative which was taken to provide a comprehensive legal framework. To some extent, it succeeded in providing legal sanctity and safeguarded e-commerce within its local or trans-border spectrum.

Unhappily Pakistan is one of such fewer territories where cyber laws are still underway. However, to achieve this task is raising a number of questions. Pakistan has become a breeding place for criminals who are moving freely in our territory; resultantly cyber-crime is ascending continuously with the exponential growth in usage of mobile phones and saturation of internet.

Hence the newly born electronic banking is at great hazard in Pakistan. Hackers are posing a great time to the e-banking customers and account holders who are losing their money due to fraudulent transactions committed via internet. Criminals attacked from far-fetched places while we are suffering from juridical backlog and having no law enforcing agency to surrender them. Majority of legal experts' advice that electronic baking must be abandoned until laws are implemented. The former President, Pervaiz Musharaf on 31st December 2007, enforced Prevention of Electronic Crimes Ordinance (PECO) 2007. It was assumed as a blessing in the present need but unfortunately, it could not be passed from the parliament and was abandoned after fulfilling its constitutional life. Thus, it lapsed in November 2009 leaving the whole nation to survive in lawlessness of cyber space. Therefore, many cyber crimes are neither reported nor tried before a court of law and the criminals are not punishable under any law.

"In the absence of PECO, we use Electronic Transaction Ordinance, 2002 as backup, but the law does not serve the purpose, trial starts at the Judicial Magistrate level and that too prolongs due to flaws in the basic structure and as a result, offenders escape"

Reported by FIA official (Dawn, 26 December, 2012)

Pakistan is one of such countries where technology is launched by external forces but is adopted by internal forces rather more quickly. As we are aware of the fact, where technology is instilled it is disguised with latent threats or risks. So it has become imperative that the parliament should make a law; backed by a driving force so that we could be able to curb electronic crimes. Nevertheless, we need a comprehensive law which is in complete consonance with the international standards:

I. It must be able to provide national security and individual protection in such a way that it should not be opposed to basic human rights.
II. It must have the capability to cope with national and global aspects of electronic crimes.
III. The provisions of enactment should clearly define the fraudulent transactional crimes committed within the domain of e-banking.
IV. Internationally recognized legal definitions of e-crimes must also be incorporated.
V. The provisions of enactment must be stretched to define clearly the exceptions that are present in various situations.
VI. It must cover the rights of individuals, business entities and stakeholders representatives. It should give protection to business strategies and must not be drafted in secrecy.
VII. It must be well drafted cyber / electronic law devoid of ambiguities which severely affect the proceedings of the trial.

6. CONCLUSION

From the above dissertation, I can conclude that it has become very necessary to make a policy framework and sophisticated legislation to cover financial and fraudulent transactional crimes, covering an entire range of e-banking crimes. It is equally important that an independent investigation agency should be established under the enactment equipped with electronic means and forensic laboratories to handle such crimes. It is rather impossible to exclude crime from the domain of cyber space but it is possible to have a regular check on banking activities and transactions. The only promising step is an independent legislation and independent investigation agency to cope the situation and the weaknesses can be remedied by enacting and implementing a strong legislation on the subject.

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 cyber crime in the existence of cyber laws.

REFRENCES

Agboola, A. A. (2006). *Electronic Payment Systems and Tele-banking Services, Journal of Internet Banking and Commerce*. Vol. 11, No. 3. Retrieved from http://www.arraydev.com/commerce/jibc.

Akhter, F. & Kaya, L. (2008). Building secure e-business systems: Technology and culture in the UAE. Brazil: Fortaleza.

Anguelov, C. E. et al. (2004). *U.S. Consumers and Electronic Banking, 1995–2003*. United States: Federal Reserve Bulletin.

APWG (Anti-Phishing Working Group). (2004). Phishing Activity Trends Report from http://www.antiphishing.org.

Balachandran and Balachandher, K. G. (2000). E-Banking Development in Malaysia: Prospects and Problems. Malaysia: 10 JIBL, 250.

Barman, S. (2002). Writing IS security Policies. Indianapolis: New Riders Publishing.

Brooks, J. (2006). Anti-Phishing Best Practices: Keys to aggressively and effectively protecting your organization from Phishing Attacks. Cyveillance: White Paper.

Choo, K. K. R. (2008). *Money Laundering risks of prepaid stored value cards.* Australia: Australian Institute of Criminology.

Denning, D. E. (1999). *Information Warfare and Security*. USA: ACM Press.

Ellison, L., & Akdeniz, Y. (1998). Cyberstalking: the Regulation of Harassment on the Internet. USA: Criminal Law Review, December Special Edition: *Crime, Criminal Justice and the Internet*, pp 29-48.

Gartner. (2007). Information Technology and Proposed Threats. Retrieved from http://www.gartner.com/it/page.jsp?id=565125

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

Kovacich, G. L. & Halibozek, E. P. (2003). *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*. USA: Butterworth – Heinemann.

Litan, A. (2004). Phising attack victims likely targets for identity theft. Retrieved from http://www.gartner.com/DisplayDocument?doc_cd=120804.

Nitsure, R. R. (2003). E-Banking: Challenges and Opportunities. London: Economic and Political Weekly Report, Vol. 38, No. 51/52. pp. 5377-5381

Steiner, T., & D, Teixeira. (1990). *Technology in Banking*. New York: Irwin.

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. London: Electronic Commerce Research and Applications, Vol. 1, No. 3. (pp. 247-263).

Tudor, J. K. (2001). IS security Architecture, An Integrated Approach to Security in theOrganization. USA: Auerbach Publications.

US Attorney General (1999). Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President. August, 1999.

Wood, C. C. (1995). IS security awareness raising methods. Computer Fraud & Security. Washington: Bulletin (June): 13-15.

Wueest, C. (2005). *Threats to online banking*. Dublin: Symantec Security Response.

Zin, A., and Yunos, Z. (2005). How to Make Online Banking Secure. Ghana: The Star InTech.

Zuckerman, E., Roberts, H., McGrady, R., York, J. & Palfrey, J. (2010). *Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites*. Harvard: The Berkman Center for Internet & Society at Harvard University.