INTERNET BANKING AND ITS POTENTIAL RISKS

Pervaiz Khan\(^1\) and Muhammad Asif Khan\(^2\)

Abstract

Internet banking is playing pivotal role in our daily life’s working, such as paying bills, transferring funds, buying products and so on, at any time and from anywhere through usage of internet. However, it has also some cons, which need to be addressed in the future. These disadvantages include: risks to consumers’ trust; reduction in employment opportunities; and not fully equipped to control money laundering.

Keywords: Customer, Internet Banking, Privacy, Reputation, Risks Security, Trust

Introduction

Internet – the driving engine of the new economy – has gifted customers with online banking, which is one of the latest and sophisticated means of electronic funds transfer (EFT). This provides customers with cheap, convenient and speedy banking facilities of balance reporting, bill payment, rate information and inter-account transfers without leaving their homes (Daniel, E. 1999). With the support of online banking, banks and financial institutions now can offer the desired services to the customers without opening more branches (Azzouni, A. 2003). Furthermore, financial institutions’ role has become more vital with the

---

\(^1\) Assistant Professor at Law Department, Bahria University, Islamabad.
Email: pervaizkhan@hotmail.com

\(^2\) Head of Department, Department of Law, University of Malakand, Pakistan.
Email: ursasifkhan@yahoo.co.uk
rapid growth of electronic commercial (e-commerce) (L.D. Crerar, 2000). However, in spite of the significance of online banking in everyday life, due to absence of normal personal interaction between bank personal and the customer, there is constant threat to consumers’ trust – a major factor in the context of banker and customer relationships (Mukherjee, A., & Nath, P. 2003).

This paper focuses on the dimensions of consumer’s trust such as security, privacy, and reputation in the context of Internet Banking (IB). It also discusses issues such as unemployment and concealment of proceeds of crime, attached with IB.

**Brief Overview of IB**

Banking is now no longer the exclusive sphere in which the customers for checking an account or making a transfer meet face-to-face with bankers (Azzouni, A. 2003). Banks have adopted computers, internet and telecommunications for their operations. The internet ever-increasing use in our daily life and the decreasing price of personal computers/PCs have greatly facilitated the banks to offer their services online (The Law of Scotland).

The first internet-only bank in the world was established by the name of Security First Network Bank (SFNB) in America in October 1995. Its success has contributed in the emergence of numerous other online banks around the world, such as Egg and Smile in the UK in 1998 and 1999 October, respectively (Crerar, L. 2000). In Pakistan, it was launched in 2005.
Definition of IB
It refers to a system which enables the bank’s customers to access accounts and general information on given products and services through a personal computer or intelligent device.

Two Broad Models of IB
Broadly speaking, there are two models of IB. First, IB is employed by the traditional banks as an additional means for communication with its customers. Second, new financial institutions or standalone entities have employed it as their primary channel of delivery, for instance Egg Bank in UK.

Types of IB
Following are the types of IB. These types can be termed as the services provided by the IB.

Informational
This is the basic level of IB where the bank markets information about its products and services on a stand-alone server.

Communicative
In this level, there can be limited interaction between the customer and bank regarding electronic mail, account inquiry, loan application or static file updates.

Transactional
In transactional online banking, the customer can execute transactions including accessing accounts, paying bills, purchasing products and transferring funds.
Potential Risks to Consumer’s Trust & IB

Internet gifts banks with ample opportunity to gain competitive advantage in the provision of services to customers, but this goal can only be achieved if there is sufficient customer migration to online banking (Fock, S. T., & Koh, H. C. 2006). To achieve this end, clients’ trust plays pivotal role. Similarly, unless consumers do not trust new technology or facility, they are reluctant to use it (Howcroft, B., Hamilton, R., & Hewer, P. 2002).

Trust means the ‘willingness to rely on an exchange partner in whom one has confidence’ (Moorman, C., Deshpande, R., & Zaltman, G. 1993). Spekman says it is the cornerstone of strategic partnership between the bank and its Internet user (Spekman, R. E. 1988). In the context of IB, trust means the reliance of consumer confidently on the online bank activities in online environment. Because of the physical separation of the bank and its consumer, its role even in virtual world becomes more important than in the real world. However, as will be discussed below, the factors, that contribute to building consumer’s trust in online banking such as security, privacy and reputation, are not fully free from risks.

In order to elaborate the issue of consumer’s trust in ‘IB’, the essay will individually discuss the dimensions of the trust, which is also given in the following figure no-1.
Fig.no.1.
Development of Relationship Between Bank and Its Customer (online User)

↓
Consumer’s Trust
↓
Dimensions of Trust
↓

_________________________________________________
↓          ↓           ↓           ↓            ↓
Security  Privacy    Reputation   Ethics    Info.Asymmetry

Security Risk
The burning issue for experts and internet analysts relates to the security of the network on which business is being done. The IB, which occurs in ‘open’ networking system, exposes the system for interference from third parties (Crerar, *Stare Memorial Encyclopedia*, 277, para 386). Consumers sometimes believe that the internet payment channels are not secure and can easily be interrupted. For instance, in Pakistan, during the month of Ramadan, few days before Eid festival, people normally prefer waiting many hours for shopping in the polluted and crowdy environment, rather availing the facilities provided by online banking. Some customers prefer TCS (A courier company in Pakistan which performs couriers, shipping, packaging and selling services), over online banking facilities, as they are reluctant to compromise their financial information in term of credit card numbers (Faisal, Khan, 2005). Apart from educational and language threat, security is one of the major threat.
linked with online banking in Pakistan (Kundi, G. M., & Shah, B. 1970). Pakistani government took some initiatives, such as ETO-2000 and ECA-2007, to ensure security and build confidence of the online community, yet the authentication procedures are causing threat to the confidence of online users (Kundi, G. M., & Shah, B. 1970).

UK banks are also allegedly placing customers at a profound risk, as they cannot effectively prevent hackers or fraudulent limitations of their sites. Mikko Hypponen, F- Secure’s Chief research officer, said that hackers are stealing money of other online consumers by using such a virus, which even cannot be detected by anti-virus system. In April 2005, there were 54 separate phishing attacks, happened in the UK. Phishing is a scam where criminals send fake e-mails to trick the customers into revealing their accounts. To counter the problem, different banks such as Halifax and Barclays have introduced the security measures and decided to introduce delays in some electronic transfers. But these delays, which banks will use to investigate unusual transactions, may likely adversely affect customers’ interest into online banking. Laurence Baxter, a senior police-advisor at consumers association said that ‘they could do more on security if they need to. But they cannot use this as an excuse to sit on people’s money for days on end’. Likewise, in March 2005 “British police revealed that they had foiled a cyber crime gang’s bid to steal $412 million from the London offices of the Japanese bank Sumitomo” (CNN News, www.CNN.com).

In the USA, a Miami businessman capital had been transferred from his account (in the Bank of America) by the fraudster accessing the account details of the claimant through a key-loging virus. Bank Protection Act of 1968 requires banks to adopt basic security procedures and devices to
discourage robberies, burglaries and larcenies and to assist in the identification and prosecution of persons who commit such crimes. There is Bank Protection Act of 1968, but it does not define how this law might be applied to electronic banking and to what extent could it be used to require ‘encryption’ aiming to protect against misuse of confidential information (Boger, W. H., & Tufaro, P. S., 1997). Similarly, The Financial Right to Privacy Act is a law that protects bank customers from unauthorized government access to their financial records; a strict application of Financial Right to Privacy Act in the electronic banking environment could create a classic conflict for banks protecting customer privacy against the government’s actions to track suspicious transactions for law enforcement purposes (Boger, W. H., & Tufaro, P. S., 1997).

Some technologists say that new technology such as encryption or digital signatures may resolve security problems that could boost consumer’s confidence. However, many banks are facing problems in implementing these developments into network practice (Crerar, *Stare Memorial Encyclopedia*, 277, para 386). A. Azzouni says that most of the banks still rely on user names and passwords techniques in IB systems, because of its low cost and easy implementation (Azzouni, A. 2003).

**Privacy Risk**

Privacy gives us a fundamental right not to have our lives interfered with, and this right is also enshrined in the European Convention of Human Rights. One of the most important duties of the banker to its customer is to maintain confidentiality in relation to customer’s affairs (Azzouni, A. 2003). However, consumers have concerns about privacy violation and lack confidentiality in online banking system, which could be resulted
from the misuse and the lack of control of personal information after transaction (Hoffman, D. L., Novak, T. P., & Peralta, M. 1999). Barclays also once stopped its on-line operations, as customers alleged that others could read their accounts. Due to the emergence of latest technologies, it becomes easy to collect personal information of the consumers and to share it with third parties (Clay, K., & Strauss, R. P. 2000).

The internet by its very nature facilitates the right to privacy. This is because the user mostly remains anonymous. Natasha Jarvie says ‘Anonymity protects our privacy by preventing others from determining what we do virtually or what we say on network’. (Jarvie, N. 2003 110-115). However, it should be mentioned here that the hacker, infringer or offender is also one of the users of the internet, as well as anonymous unless arrested and produced before the court of law. Simply put, IB does not provide its customers with absolute privacy (Jarvie, N. 2003). Meaning hereby, privacy, an antecedent of consumer’s trust, is not fully safeguarded in online banking systems.

Indeed, sometimes, the so-called limited privacy right of the consumer in online transactions cannot be maintained. Normally, banks use cookies for IB services. British Bankers Association (BBA) says that cookies are essential part of service in occasions such as e-banking or security. Banks such as Barclays, HSBC, Lloyds TSB and Citibank use different kinds of cookies. As per recitals 24, 25 and art 5(3) of the Directive on Privacy and Electronic Communication (DPEC), a cookie may be used for legitimate purposes, providing the concerned user with clear and comprehensive information about the purpose of processing and offering him a right to refuse cookie (Munir, A. B. 2004).
The UK has implemented DPEC through Privacy and Electronic Communication (EC Directive) Regulations 2003. Considering second part of art 5(3) of the Directive, the UK has made an exception to the provision of clear information to the user and his right to refuse the cookies, if the sole purpose is to carry out or facilitate the transmission of communication (Munir, A. B. 2004). In other words, the cookies can be placed in the hard drive without the permission of the user, which is termed as a violation to user’s privacy rights. As Iain Bourne, the strategic policy manager at the information commission said that ‘there is a basic transparency problem, but we think that if someone uses a cookie (or similar device) that profiles the user, then it is an invasion of privacy. Users should have the right to say no’ (David Neal, 2003).

Sometimes, consumers in the US have also been reluctant to conduct transactions over the internet, due to money safety concerns and privacy concerns in relation to personal information including financial records (S. H. Willam 1996). There is Electronic Funds Transfer Act (EFTA). The EFTA defines the rights and liabilities of customers and financial institutions that use electronic systems to transfer funds. The EFTA includes rules governing the issuance of access devices, liability for unauthorized transfers, disclosure of terms and conditions of use, documentation of transactions, and procedures for resolving errors—all with the objective of protecting individual consumer rights, but its application in new electronic transactions could amount to unreasonable costs, and create excessive and unnecessary paperwork (Boger, W. H., & Tufaro, P. S., 1997). Likewise, different technologies have been adopted by the banks in Pakistan for consumer’s privacy protection, yet a number of incidents compromising consumer’s privacy have already been happened (Kundi, G. M., & Shah, B. 1970).
Risk to Reputation

Reputation is another dimension of trust in online banking. The customer normally considers bank’s reputation before sharing its information with it. Customers are always reluctant to use those online banking facilities, which have poor reputation (Ba, S. 2001). ‘The bank should be constantly aware of the factors such as user-friendliness, efficiency and speed of its service, the inadequacy of which can damage its reputation’ (Crerar, The Law of Banking in Scotland’, 489). Security and privacy risks do contribute to the bad image of a bank. A bank can also suffer reputational loss if it fails to provide a system to cope with demands of the customers.

Risks Linked with Other Dimensions of Trust (Such as Ethics and Information Asymmetry)

Ethical values determine the chances of banks giving incomplete information about product or divulging confidential information about customers. It is also one of issues, attached with ‘e-Business’ in Pakistan (Kundi, G. M., & Shah, B. 1970). Ethics and honesty, important aspects of good business morality, help in building trust in a broader sense (Humphrey, J., & Schmitz, H. 1998).

Information asymmetry is also one of the factors, which can affect customer’s trust. One of the important features of online shopping from consumer’s perspective is the access to quality and complete information on products and services (Joseph, M., Sekhon, Y., Stone, G., & Tinson, J. 2005). But complete information about the quality of products is difficult or sometimes even impossible to obtain in the virtual world (Klang, M. 2001). In virtual world, customers have limited chances to meet the seller to discuss the quality of the product. Thus, comprehensive
assessment of the product may likely remain incomplete before making transaction decision.

Unemployment, Computer Literacy, and Concealment of Crimes/Liability

As will be discussed below, there are other issues such as unemployment, computer literacy and concealment of crimes, which are attached with online banking.

Risk of increase in Unemployment

Though online banking facilitates its customers with cheap, convenient and efficient banking opportunities. However, it also contributes to the increase in unemployment, or decrease in jobs. This is because IB depends on computers network through internet, limiting people physical involvement. For instance, almost all online banks have home pages available on internet, facilitating customers in availing services such as shopping without involving physically or personally with the seller. This replacement of human labour with machines contributes to increase in unemployment. Indeed, an increase in the use of online banking is likely decreasing banks’ branches, in turn, further increasing unemployment. It should be mentioned here that unemployment is one of the causes for societal problems, especially in poor economies. For example, Pakistan, a weak economy, falls within the lower groupings of the United Nations’ Human Development Indicators (2015). Currently, 45.6% of its total population is living in multidimensional poverty (Human Development Report, 2015). The country is facing terrorism issues for more than a decade, and lack of proper employment opportunities is one of the reasons for terrorist activities in Pakistan. This makes important for the country to create maximum jobs for its nationals. Simply put, online banking
amounts to decrease in employment opportunities, in turn, contributing to societal problems.

**Lack of Computer/Internet Literacy**

To avail the facilities provided by online banking, a customer should know about the basics of internet. IB is not a blessing, rather a potential threat for those who have no knowledge of internet. This is because those with limited knowledge of internet are not sufficiently capable to make proper use of online banking services. Thus, while using IB, they may negligently cause problems to themselves. Such as in form of transferring the money to wrong persons or making payments for the un-wanted products. There are tools, which redress customers’ concerns. However, it is time-consuming and tiredly.

**Risk of Securing the Process of Money laundering**

Generally, the term ‘Money laundering’ is used to describe the process that covers the source of money (Ellinger, E. P., Lomnicka, E., & Hare, C. 2011). Leong says that it is the process by which a ‘Dirty Money’ after a cycle of transactions is turned into washed, clean and legal money (Leong, A. V. M. 2007). It allows the criminals to maintain control of the proceeds of the crime and avoid detection (Leong, A. V. M. 2007). Money Laundering is considered as the world’s third largest industry after internal oil trade and foreign exchange (Robinson, J. 1998). In fact, after 9/11 attacks, in addition to tax evasion and frauds, financing criminal activities have become one of the major purposes of Money Laundering (Ryder, N. 2007).

Sometimes, criminals and tax evaders also use internet and/or electronic funds transfer to conceal the proceeds of their crime or taxable assets
(Crerar, ‘Stare Memorial Encyclopedia’, 277, para.386). In fact, it has found that even terrorists are using new electronic technologies to transfer money over the internet to hide their true origin (Ping, H. 2005). A launder attempts to dodge the detection process through changing and sending money in electronic form (Simser, J. 2008). Criminals have used traditional banks as a safe passage to launder money; however, IB has made this job even easier for them in relation to their location and prosecution (Schepp, D. 2001). The worldwide access to detect fraud is complicated, as it is difficult to identify the place from where the account is actually accessed (Schepp, D. 2001). For instance, in spite of the progress that has been made since the new regime on ‘Defusing the ID Issue’ in April 2004, the UK authorities do “not yet” have an effective framework to trace all Money Laundering cases (P. Robinson, 2005).

Conclusion

Internet banking has brought a revolution in the modern banking system, where people have become more at ease in conducting their daily transactions in the virtual world. Customers can access banking facilities or services 24 hours and 7 days from their homes. However, there is constant threat to clients’ trust in the context of online banking. There is possibility of compromising different dimensions of customers’ trust, such as security, privacy, ethics and communication, in online banking system. In addition to this, internet banking is contributing its part in the increase of unemployment, in turn, amounting to societal issues. Moreover, online banking system is not fully equipped to counter money laundering. The afore-mentioned issues need to be addressed for further development of internet banking in the future.
References:


Crerar, *Stare Memorial Encyclopedia*, 275, para 381.

Crerar, *Stare Memorial Encyclopedia*, 277, para 386.


CNN News. Companies at risk from cyber-crime, Available at: www.CNN.com.


70