

A ETHICAL ISSUES IN e-BANKING – ITS ROLE & IMPACT

G.DAVID RAJU

Asst Professor, Dept. of Business Administration, KBN College PG Centre, Vijayawada, A.P., India

Abstract— Ethical issues in the financial services industry affect everyone. The public seems to have the perception that the financial services sector is more unethical than other areas of business because the industry itself is quite large. It encompasses banks, securities firms, insurance companies, mutual fund organizations, investment banks, pensions funds, mortgage lenders—any company doing business in the financial arena. Because of its vast size, the industry tends to garner lots of headlines, many of which tout its ethical lapses. Moreover, Technology is ever growing and we are encountering tools that are beneficial to the general public, but in the wrong hands can create great controversy, breaching our basic right to privacy, respect and freewill. Active presence in electronic trade market has become vitally necessary owing to two pervasive transformations resulting from information-communication technology and globalization revolution, adding to the significance of an efficient banking system which can enable confident financial transactions for electronic users. This responsibility is undertaken by electronic banking system. Since electronic banking is still undergoing development and transformation, little experience is available regarding presence of ethics principles in this field: nonetheless, due to undeniable role and importance of this technology in fiscal and monetary tasks, it is essentially vital to identify the factors affecting the ethics principles aimed at resolving the associated problems. Thus, taking into account the significance of ethics in electronic banking and its ascending trend across the world and besides analyzing one of the most important upcoming challenges of electronic banking, the current paper it is attempted to propose model which is capable of monitoring ethics issues in electronic banking and provides the grounds for encountering them consciously.

Index Terms— Electronic Banking, Upcoming Challenges, Ethics issues of Electronic Banking.

I. INTRODUCTION

As technology evolves, many Internet applications become so popular. Online Banking (sometimes called the Internet banking or e-banking) is one of the Internet applications which have major impact on our modern life. The benefits of Online Banking (e.g. easy-to-use, convenience, fast, cost-saving) for both banks and Internet users make Online

Banking so popular around world. Online Banking has changed the way how the traditional banking industry interacts with banking customers. There is no doubt Online Banking is one of the most sensitive tasks performed by the Internet users. Although banks have strongly encouraged their customers to do Online Banking and advertise the Online Banking is very safe and secure, apparent this is not true. Claessens discussed many security issues related to Online Banking 2. Also in Lampson's "computer security in real world"¹, he pointed out that in general the most computers in real world are not secure because security is too expensive.

Moreover, the communication via the Internet has made computer security very hard¹. In fact the end users' PCs are weakest link of online applications. According to Lampson's "money talks" concepts for security, to make the banks/companies profitable, even sometimes the banks/companies learnt the inadequate security in their current systems, compared between the low risks of potential loss and high cost of security, the banks/companies may not want to upgrade their current security system¹

And new ethics issues arise. Since electronic banking is still undergoing development and transformation, there is only little experience concerning presence of ethics principles in this scope (Dr. Lisa Harris, Dr. Laura J. Spence, 2002) and there are still many doubts about extent of impacts of this technology on ethics. Although economical and organizational advantages of this novel technology cannot be doubted but there is generally a doubt concerning the style through which information technology transforms the social scope and especially the ethics issues (Dr. Babak Sohrabi, Amir Khanlari, 2009).

Meanwhile observance of ethics principles in any subject and field is highly important and can never be neglected in the scope of personal and social life of people (Gholami, 2009), ethics issues particularly become further important when pertaining to financial and monetary tasks. Electronic banking, as one of the new subjects having both technological and financial aspects, is considered as the focus of concerns for attracting observance of ethics principles in the modern times; this subject has preoccupied the minds of considerable number of ethics-in-engineering thinkers

II. ETHICS IN ELECTRONIC BANKING

It can be imagined that users of information technology face endless ethics problems; the problems which specifically arise in connection with gaining profit and creation of value for society (Paulet, 2011). Under these conditions, it becomes necessary to reprocess and re-define the ethics principles, objectives, and values. The users intend to be committed to observance of ethics and assurance of social justice along with guaranteeing growth of electronic banking system and promotion of quality of bank services by using more resources. So, the relations of banks with each other as well as relationships among organizations, customers, and personnel shall be rethought (Chowdhury, 2011).

III. ETHICS IMPACTS OF ELECTRONIC BANKING

Electronic banking influences level of ethics observance in different manners. The most important ethics aspects of electronic banking include:

Threatening people's privacy Electronic banking threatens different aspects of people's privacy:

1. Primarily, confidentiality and secret-keeping

It is crucially important to defend the value of users' information confidentiality including their personal details and accounts and transactions. This indicates that an impregnable connection shall be made between the sender and the receiver and people's confidential information shall not be disclosed (Dr. Hussein Bashir, Muhammad Reza Herati Nik, 2011). It is noteworthy that the customers of electronic services will be displeased if they find their own information in another marketing list.

Issues such as data exploring, registration of click trace on the web and other items have caused new challenges with regard to privacy in electronic banking (Bynum, 2001).

2. Right of protection and non-intervention

On this basis, access to the data are specified according to rights of individuals (Dr. Hussein Bashir, Muhammad Reza Herati Nik, 2011) and since any deal either commercial or non-commercial requires money transfer and payment and this transaction is undertaken by electronic banking, the banks can therefore monitor all activities of their customers. However, it is not acceptable and ethically descent to detect and explore customer's information without their permission. Nonetheless, electronic supervision of operators on personnel shall be defined according to law and the personnel must be also able to have access to information of other people in legally permitted cases.

Identity verification is a process which determines whether a person or object is the same stated thing or individual or not; in this process, it is assured that the confirmer of statement or person will not be able to deny the assertion in the future (Dr. Hussein Bashir, Muhammad Reza Herati Nik, 2011). Of course, it must be noted that this obligation to protect privacy

and namelessness is not supposed to facilitate illegal and undesirable activities with the aid of computers and shall not help moneylaundering and similar activities, for example (Marzieh Dowlatabadi, Zahra Khazaie, 2009).

3. Security Protection

In the age of computers, with presence of viruses and international espionage by hackers who work from thousands of kilometres away, security protection is clearly a discussable subject in the scope of electronic banking ethics (Seghatoleslami, 2009). This concept in the scope of electronic banking signifies protecting information against non-permitted use and access, inappropriate changes, robbery, and data damage or destruction (Dr. Hussein Bashir, Muhammad Reza Herati Nik, 2011). Variety of malwares and/or programmed threats causes serious problems in computer security especially in financial and monetary areas. These software threats include:

Viruses that cannot by themselves be executed and need to enter computer programs; worms which are able to transfer from a machine to another all over the networks and might execute part of themselves on different machines. Trojan horses which appear in the form of a program while damaging the system by hiding under this appearance; logic bombs that analyze certain conditions and are executed if such conditions are provided; Computer crimes like embezzlement or planting logic bombs usually are committed by trusted individuals who have the permission to use the computer systems in banks (Bynum, 2001). In addition, hackers check the computers without permission; some of them steal or damage the information and others investigate the systems merely for getting aware of their mechanism and information content (Marzieh Davudabadi, Zahra Khazaie, 2009).

4. Data Manipulation and Financial Cheating

Data deformation is a form of data manipulation and includes changing data in a data-base. Data manipulation includes addition, elimination or alteration of data in the database and is generally aimed at changing financial data which leads to rendering improper financial statements or other unreal fiscal reports. This would result in mistakes by many individuals including those inside an organization or outsiders who use this information for making important decisions (Dr. Ramezanali Royaie, Jamal Bahri Sales, Asgar Pakmaram, 2010).

5. Error Occurrence in Financial Transactions

This includes error in transactions of debt and credit accounts resulting from human mistake or might occur because of functional profit or presence of software bugs.

6. Health and Safety

Health and security concerns are among other problems of electronic banking for both personnel and customers; remarkable failure might be followed in the field of electronic banking if these problems are not taken into mind and no solution is devised for coping with them. Attempts to establish arrangement with electronic banking and doing activities in certain time and at high speed might cause stress for some

customers or could endanger their health due to immobility or radiations from computer monitors (Marzieh Davudabadi, Zahra Khaza'ie, 2009). Also, if people are encouraged to shop from their area of residence and work in the same place and if all activities require money transactions which are performed by electronic banking, thus adverse psychological consequences such as depression and solitude can arise and lack of social contact and relations might damage their ethics, social, and cognitive developments (Hassan Pour Ghoroghchi, 2007).

7. Unemployment caused by electronization of activities

In the current world of computers, their exceeding growth as well as speed, precision, and lack of tiredness compared to humans have made them a threat to occupations leading to economical motives for replacing manpower by computer devices.

These days, many bank clerks, telephone operators, security guards, etc have been substituted by computer operators.

IV. ROLE OF ETHICS IN BANKING

Ontologism based on the concept of good as opposed to evil helps us define the banking business from the point of view of ethics. The idea of awareness or conscience of the need for banking products or services inevitably comes to mind. This simplified parallel leads us to the conclusion that full awareness of and the related ethics about the importance of banking products and services is imminent to all economies, regardless of their economic development.

The basic ethical principles in banking are:

1. Principle of mutual trust is of special importance for successful functioning of the business system. Important and valuable deals are very often contracted over the phone, in the absence of witnesses, while the relationship between the participants is dominated by the inviolable principle of mutual trust.

2. Principle of mutual benefit and interest means that none of the partners in a business relationship should feel cheated;

3. Principle of good intentions is very important for business ethics and moral behaviour. This principle means that there is no intention to treat the business partner in an immoral way, whether it refers to deception, theft or some other undesirable way of treating a business partner;

4. Principle of business compromise and business tolerance refers to the harmonization of the conflicting interests of participants in the business process;

5. Principle of ethical improvement of business behavior represents the business partner's readiness to accept the mistake that has been made as a result of his own actions.

He should admit the mistakes and respond in an appropriate way;

6. Principle of de monopolization of one's own position, because monopolistic behavior on the market does not contain any ethical market value and

7. Principle of conflict between one's own interests refers to the inability to relate common to personal interests, with simultaneous adherence to the same ethical values.

The violation of ethical principles in banking occurs when the lenders take too much risk, trying to find a loophole that allows them to approve more loans. Strict adherence to the law and regulations in the field of banking makes it possible to grant loans to all the qualified clients in a fair way.

The theoretical assumption that banks with higher capitalization rates and a better liability structure can enter long-term credit arrangements with a higher risk level has been empirically proven. It stems from the above that each bank should respect the general and the specific principles in formulating its credit policy. Since banks are trying to optimize their micro economy, they perform a significant macroeconomic function through their activity. The bank's non-objectivity is most evident when it comes to establishing accurate information about the character of the debtor. Based on its subjective evaluation, the bank makes conclusions about the debtor. This indicator is most obvious when it comes to personal loans, and less obvious when it comes to corporate loans.

The analysis of every loan application requires one or several loans officers who have contacts with the client, one or several analysts who evaluate the client's financial abilities, a board for loan approval or a loan administrator who finally approves or rejects the loan request.

By protecting themselves, the banks also protect the efficiency of using the macro system's accumulation. In this way, the loss of banking and financial resources in the macro system is restricted and the selective and allocate functions of the total system are improved. A bank is liable to run business books in compliance with the banking chart of accounts, preparation of bookkeeping documents, evaluation of assets and liabilities, drafting of financial statements in accordance with applicable regulations and professional standards (the Central Bank may prescribe, for the purpose of public announcement, a type, form and content of statements, method and deadlines for their publication). A bank must organize the internal audit which should conduct its activities in an independent and impartial manner, and contribute to the development of the bank's operations through its advisory services. The internal audit of the bank's operations should conform to the operating principles and business ethics code pertaining to internal auditors. In its work, the internal audit should harmonize the methods of its work with the work of external auditors. The person in charge of internal audit tasks should not be involved in other activities within the bank. If the internal audit unveils any case of illegal operation and violation of the risk management rules in the course of its

inspection of specific fields of bank operations, it must promptly inform the bank's management thereof. If it fails to do so, the bank is running the risk of becoming illiquid, insolvent and its operations insecure.

Banking business is attractive for illegal transactions only if the effectiveness of a controlling mechanism for a consistent conformity with the operating principles is missing. Continuous monitoring is a significant activity for banking operations, since the very nature of this activity involves a rapid change along with innovations. In traditional banking activities this problem is clearly seen, since some sort of records is kept on transactions.

However, there is an obstacle in the e-banking domain, particularly in regard to detection of illegal money transfer from an account to a card with a deposit amount.

It is to be expected that a more extensive use of e-money will lead to an increasing misuse of ethics. Even though banks, financial companies and clients gain multiple benefits by using the e-banking system, at the same time the application of e-banking jeopardizes the ethical domain, since it gives rise to increased cybercrime. Hackers usually disrupt the operation of information systems and transfer financial funds to their own accounts.

The most common targets of such criminals are ATMs. It is not to be neglected that banking technology is getting better, but hackers also develop their skills to steal funds from banks and thus undermine legitimate banking transactions. In order to prevent the identity frauds, legislative institutions notify the clients that they safeguard the sources of private information. Bankers should provide more detailed instructions to clients to check the balance on their accounts at least once a month and to report immediately any observed irregularity. Owing to the introduction of e-banking services, clients can check their account balances on a daily basis. Electronic business is possible to apply only if a mechanism for securing financial and other transactions on the Internet is developed. By using encryption systems and digital certificates it is possible to realize four basic functions of the transaction security, such as: confidentiality, authentication, integrity and incontestability. The efficiency of such measures should be proved by more extensive use of electronic money. The most important benefit of e-business is that financial flows assume different profile, whereas the banks move their desk operations to the clients' computers. Time will show whether we will reach statistical figures from the developed west where more than 80% of transactions are affected electronically.

V. CONCLUSION

Spread and fast influence of internet and technological advances particularly in the scope of information and telecommunication technologies, the financial services, and banking industries have transformed the service provision

channels used in these areas. With progress of aforementioned technologies, electronic trade promises a new revolution; in fact, the widespread belief is that impact of electronic trade enables banks to provide a cheap and direct way for information exchange as well as product and service deals for businesses in general, and, for customers in particular. Also, successful growth and development of electronic banking requires identification of challenges encountering electronic banking (Sedeighe Khorshid, 2009). In the current paper along with analyzing one of the most important upcoming challenges of electronic banking, it was attempted to propose a model that is capable of monitoring ethics issues in electronic banking and provides the possibility for dealing with them consciously.

Based on the findings of the current research, the individuals, organizations, and banks using information technology are recommended to present a strategic program for resolving ethics problems and issues discussed in the present research.

VI. REFERENCES

- [1] B. Lampson, "Computer Security in the Real World", IEEE Computer 37:6, 37-46, June 2004.
- [2] J. Claessens, V. Dem, D. Cock, B. Preneel, J.Vandewalle, "On the Security of Today's On-line Electronic Banking Systems", Computers & Security 21(3), pp. 253-265, 2002
- [3] Hole, K.J.; Moen, V. Tjostheim, T., Case study: Online Banking security, Security & Privacy, IEEE Volume 4, Issue 2, March-April 2006 Page(s):14 – 20
- [4] Aladwani AM, 2001. Online banking: a field study of drivers, development challenges, and expectations. International Journal of Information Management 21, 213-225.
- [5] Alipour LA, 2011. Electronic Banking and Revision of Consumption Pattern, MELLI Bank Journal, 1-5
- [6] Bynum TW, 2001. Computer Ethics: Basic Concepts and Historical Overview. Ethics and Information Technology, 109-112. Intl. J. Manag. Human. Sci. Vol., 2 (S), 1127-1132, 2013 1132
- [7] Chowdhury MM, 2011. Ethical issues as competitive advantage for bank management; Humanomics , 27 (No 2), 109-120.
- [8] Christian B, Joe C, 2001. Planning for electronic commerce strategy: an explanatory study from sector. Logistics Information Management; 14 (1/2), 24-32.
- [9] Dospinescu O, Rusu D, 2004. The adoption of electronic banking services in developing countries – The romanian case; Department of Business Information Systems, 20-35.
- [10] Dr. Lisa H, Dr. Laura J, 2002. The ethics of banking; Journal of Electronic Commerce Research, 3 (2), 59-66.