Internet Banking Law: An Iranian Perspective
Problems and Prospects of Introducing Islamic Microfinance in Azerbaijan Republic

Mostafa Elsan *

Received: 12 Mar 2009 **Accept: 1 Jun 2009**

Abstract

Bank supervision and monetary policy are strategic concepts in the economy of countries. Development of electronic communications, especially in online and international spheres, has largely threatened financial services in view of security and illegal access to banking networks. Anonymity and identity theft has endangered electronic commerce by crimes like phishing, fraud and different types of unauthorized access. However these probabilities which sometimes become true have not stopped developing fleet of World Wide Web. In fact successful experience in internet banking indicates the necessity of use of new technologies to facilitate and expedite electronic commerce. In this paper, different legal aspects of internet banking have been analyzed briefly from Iranian law perspective.

Keywords: Internet Banking, Iranian Electronic Commerce Act, Phishing, Supervision and Monetary Policy.

JEL Classification: O31

---

* Ph. D. (2007-Private Law), University of Shahid Beheshti; Faculty Member, Tarbiat Moalem University of Azarbijan, Iran.

1- Introduction

Although using electronic means of communication was prevalent in banking industry, but the globalization of internet lead to "electronic commerce". Due to its facilities, the thought was supported that the bankers can use electronic communications in an unlimited environment of internet. Obviously in the global commerce, these technical possibilities were hardly acceptable from the view of law and national economy.

Electronic payment methods have been resulted in convenience and cutting the costs whereas its novelty and some ambiguous view points on its insecurity feature is remained. Fundamental problems are arising whenever the payment systems have been developed over borders by transnational companies and via internet. Prima facie, some issues like sovereignty of states, application of the roles of central bank in these areas, control of money, foreign currencies and transactions are in conflict with international internet banking. Many of these problems are derived from unfamiliarity of legal systems and ignorance to the importance of monetary and financial policy for the states.

In this paper, legal aspects of internet banking have been reviewed by using the comparative point of view and finally some guidelines have been presented to Iranian Islamic banking system to use these new inevitable means for banking services.

2- The Concept of Internet Banking

Appearance of internal networks and international webs supported the idea of possibility of commerce via internet. So the financial and banking

in the same line are considered as essential and complementary to progress. The abilities of computers such as a two way communications and visual face to facing that was not available in television and telephone have made confidence about accuracy and reliability of internet commerce. Nevertheless some uncertainties like anonymity, identity theft and endangering the role of central banks, still remain.

In simple internet banking, an entity who has banking permissions, is designing a website by means of it, the customers could have transactions with bank and they can do many of the banking affairs. Internet has allowed a number of totally new services such as "digital money", "electronic check" and "internet cash", which provide feasible and easily access for customers all over the world.[1]

In Iran, according to Article 10 of 4th development program, the government should establish electronic banking system and should provide national and international electronic monetary services in all banks and for all customers. This shows the importance of the role of new communications in financial and monetary system of the country. Notwithstanding, internet banking as mentioned, have some legal ambiguous aspects which can lead to some restrictions in the extent of its development. In the following pages, this problem will be considered exactly.

3- Contractual Aspects of Internet Banking

There are many forms of contracts in internet banks' process of doing affairs. At least, a contract between a bank and a customer and other

---

1- Giannakoudi, Sofia, Internet banking: The digital voyage of banking and money in cyberspace, **Information & Communications Technology Law**; Oct 1999. p. 207.

contract between the bank and ISP[1] can be supposed. Such contracts don't have any new features from the view of contract law.

In internet banking, a standard form of contract is signed online by customer by clicking on the icon of "submit" or "I agree". Thus in an internet banking contract, general provisions "are completely formulated by the bank and they will be interpreted against the bank by the judge in the event of a dispute".[2]

In the contract, the bank has obligations to making available all of its internet services and process of orders for customer through online communication. To secure this process, the bank should have encryption technologies and data-processing facilities which are updated and improved suitably according to the new needs of information technology (IT).

Reciprocally, the customer admits obligations according to his contractual submission, including making precautions to protect his confidential information in order to prevent fraudulent use by unauthorized persons. Furthermore, the customer is bound by all effects of contract from contract law perspective, containing performance of his obligations on behalf of bank, payment of money or providing credit to operate his account and etc.

1- "An Internet service provider (abbr. ISP, also called Internet access provider or IAP) is a business or organization that provides consumers or businesses access to the Internet and related services. In the past, most ISPs were run by the phone companies. Now, ISPs can be started by just about any individual or group with sufficient money and expertise. In addition to Internet access via various technologies such as dial-up and DSL, they may provide a combination of services including Internet transit, domain name registration and hosting, web hosting, and colocation". See for more information: wikipedia.org

2- Magnin, Cedric J, Telebanking Contract in Swiss Law, ILSA Journal of International & Comparative Law, Vol. 8, 2001-2002. p. 86.

In relation to ISPs, due to their abilities to dictate the online environment in which their customers are operating through the use of written control policies and guidelines and their capacity for screening materials on the network automatically,[1] the bankers shall contract with an ISP as a bridge between them and customers. Because the ISPs prefer to be in the position of distributors in the process of internet commerce, their liability in financial crimes may depend directly on the content of the contract between them and the banks. Although it is difficult to generalize ISPs into one group considering the different services rendered by them,[2] but in all types of service contracts, the ISP could be held liable for its misdeeds. Of course, the contractual liability for ISP may arise from an implied warranty of serviceability by the action of breaching service agreements.[3]

The changeable nature of new environment of banking may affect the content of contract between internet bank and ISP or customers. It is not the case in Iranian law, according to Article 219 of Iranian Civil Code which reads as follows , "Contracts made according to law are binding on the parties or their substitutes, unless they have been cancelled by mutual agreement or for some legal reasons". In internet, the content of contract could be changed in the direction of its security and be completed in conformity with new requirements and changes. Of course these changes should not affect vested rights or any provisions for consumer protection.

1- Zhao, Yun, Internet Service Providers and Their Liability, Law Technology, Vol. 34, 1st Quarter 2001. p.2.

2- Luftman, Douglas B, Defamation Liability for online services: The Sky is not Falling, George Washington Law Review, Vol. 65 (6), 1997. p. 1096.

3- Zhao, op. cit, p. 4.

4- Security of Internet Banking

Security of system is a primary fear in internet banking because in the internet, there is no interface and original presence and thus someone may break legal lines and become appear in the position of authorized person. Furthermore, data and information which are stored in an electronic form are subject to manipulation or destruction, either intentionally or unintentionally.[1]

Usually, the customers expect that banks protect confidential data and provide reasonable measures fitted with new threats in the new environment. For safeguarding the confidentiality of information, the internet banks stipulate in their contracts with customers, ISPs, employees and other related persons, their obligations to protect the system and nondisclosure of private information to others.

In the other hand, banks are using (a) preventing measures, including cryptography, online authorization, supervising and monitoring by a central operator; (b) detection measures such as transaction traceability and monitoring, interaction with a central system and (c) containment measures, including limits on the value stored, expiration dates on devices and on values, registration of the identity of the users with the issuer or central authority.[2]

In Iran, Article 2 (i) of Electronic Commerce Act [IECA][3] defines" secure method" as follows:

---

[1]- Douglas, John, Cyber banking: Legal and Regulatory Considerations for Banking Organizations, North Carolina Banking Institute, Vol. 4, 2000. p. 75.

[2]- Report of the Task Force on Security of Electronic Money, USA 1996; Giannakoudi, op. cit, p. 208.

[3]- Iranian Islamic Parliament approved the Electronic Commerce Act on January 7th 2004. This implicates interest for fighting underdevelopment which didn’t have typical

"A method to authenticate the correctness, the origin and the destination of a "data message", along with its date and to detect any error or modification, in communication, content, or storage of a "data message" from a certain point. A secure method is generated using algorithms or codes, identification words or numbers, encryption, acknowledgement call-back procedures or similar secure techniques".

Article 65 of IECA has defined "trade secrets" extensively, so that it includes "information, formulas, patterns, software and programs, means and methods, techniques and procedures, unpublished writings, businesses and transaction methods and procedures, strategies, plans, financial information, customers list, trade projects and the like which have an economic value by themselves".

Trade secrets have been protected in electronic commerce by imposing rules of competition and criminal law to criminals and careless persons. Article 64 of IECA reads as follows:

"In order to protect legitimate and fair competitions in electronic transactions, illegal acquisition of trade or economic secrets of agencies and institutions or the disclosure of such secrets to third parties in electronic environment is deemed an offence and the offender will be sentenced according to this Law".

---

objective supported by trade and economic sector of country. IECA, from many aspects has similarity with both Uncitral Model Law on Electronic Commerce which was adopted at 1996 (and completed with Article 5 bis at 1998) and Model Law on Electronic Signatures (2001), of course, it has some initiatives on consumer protection (Articles 33-49), protection of data messages in electronic transactions (Articles 62-65), offenses and punishment (Articles 67-77) which hadn't been predicted by Uncitral model laws. In some of these subjects, the IECA may be comparable with USA Acts, i.e. Uniform Electronic Transactions Act (UETA) and Electronic Signatures in Global and National Commerce Act (ESIGN).

Some countries have bilateral treaties to ensure on security of banking activities in international sphere. "The American-Swiss treaty on mutual legal assistance in criminal matters"[1] can be considered as an example for this cooperation. The treaty comprises frothy-one Articles. It has two aims: Controlling mutual legal assistance in general and fighting organized crimes.[2] In internet banking, it seems essential for countries and private banks to have collaboration for safeguarding security of banking and to prevent internet crimes.

5- Crimes Against Internet Banking

Due to the fact that the cost of committing financial crimes has increased by the use of advanced technologies in detecting and prosecuting computer criminal conducts, offenders promoted their skills and tactics simultaneously by employing experts in different fields of information technologies. Nevertheless, offenses against internet banking can be categorized from different aspects. Some of these offenses remain undiscovered or committed by anonymous offenders. Main types of these crimes are explained briefly in the following parts.

A- Phishing

Unauthorized access to financial information constitutes an important part of financial crimes in the internet. Phishing attacks rely upon both technical deceit and social engineering practice. In the majority of cases the phisher persuades the victim to intentionally perform a series of actions that will provide access to confidential information.[3] Thus,

[1]- The American-Swiss Treaty on Mutual Assistance in Criminal Matters entering into effect as of January 1, 1977.

[2]- Lauchli, Urs Martin, Swiss Bank Secrecy with Comparative Aspects to the American Approach, Saint Louis University Law Journal, Summer 1998. p. 874.

[3]- The Phishing Guide, NGS Software Insight Security Research. P. 5. At: www.ngsconsulting.com

phishing "is online identity theft in which confidential information is obtained from an individual".[1] User names, passwords, social security numbers, credit card numbers, bank account numbers and personal information may be kinds of secrets which have been theft and are used against the owner of such information.

As a real example, the phisher impersonate the sending authority, e.g. the online bank at which the victim has an online account and sends him an e-mail by spoofing the source e-mail address and embedding appropriate corporate logos. The e-mail recipient is likely to believe that his banking information has been used by an unauthorized person and then he attempts to reply to his mistake report. For this, he must type his confidential details to reverse transaction.[2] After this process, all such information is under misappropriation of the phisher.

Phishing often perpetrated by an organized crime. To prevent this crime, affected institutions should pursue offenders for legal remedies. Furthermore, to go update with technological changes is an integral component of a sustainable prevention.

In Iran, according to Article 2 of Iranian Bill for Punishment of Computer Crimes, anyone deliberately and without permission has access to confidential data or computer or communicational system, will be convicted to imprisonment from one month to 91 days. Therefore, to deem "unauthorized access" as a crime, it should be intentionally and without permission. About internet banking, this element seems unnecessary because it is not admissible from an offender or any financial criminal in internet when he argues that he has broken all confidential measures without intention.

---

[1]- ITTC Report on Online Identity Theft Technology and Countermeasures. P. 6. At: www.antiphishing.org/Phishing-dhs-report.pdf

[2]- The Phishing Guide, op. cit.

B- Fraud

A false representation by means of a statement or conduct made via electronic communication if it has been knowingly or recklessly in order to gain material advantages, is called "fraud" in electronic environment. In majority of countries, intentionally accessing a computer system to execute a scheme to defraud has been criminalized and will be punished by imprisonment.[1]

About internet banking, one can say that the inter-linkage between computers and circulation of large amount of monetary values through it in a short time facilitates the perpetration of financial fraud resulting in widespread and immeasurable losses.[2]

Fraud and phishing are much interconnected offenses in internet banking area which have the same prevention and prosecution measures. For prevention, the financial institutions shall imply staff education and training in technical matters, usage of superior technology of anti-spyware and cooperate with each other and with internet criminal police. Article 12 of Iranian Bill for Punishment of Computer Crimes has been criminalizing activities in which computer and communication systems have become all or partial tactics of offenders for committing fraud.

C- Money Laundering in Internet

Money laundering is defined as "a process by which the origin of funds generated by illegal means (drug trafficking, gun smuggling, corruption, etc.) is concealed. "The objective of the operation, which usually takes place in several stages, consists of making the capital and assets that are illegally gained seem as though they are derived from a legitimate source, and inserting them into economic circulation. Money

---

1- Corbett, Patrick E, Prosecuting the Internet Fraud Case without Going Broke, Mississippi law journal, Vol. 76, 2006-2007. p. 844.

2- Giannakoudi, op. cit, p. 217.

laundering is not a new phenomenon: it's as old as crime itself. Criminals have always endeavored to conceal the origin of illegally generated funds in order to erase all traces of their wrongdoings".[1] In an open environment like the internet, the exchange and transfer of money without the intermediation of financial institutions with filing records and process of transfer, it is easily possible for criminals to clean their dirty money in the cyberspace chaos.

The existence of anonymous digital cash and non controlled version of monetary values may intensify this problem. The difficulty of control, at least in theory, is resulting in other crimes like tax evasion because transacting large amounts via electronic means that leaves no paper trail eliminate records many traceable transactions and consequently limits the state authorities and police from prosecution and control.

Accordingly, the new monetary world has uncertain impacts on some legally accepted norms in the national system. For preventing or at least redressing damages arising from misuse of new technologies, it is possible to resort to traditional strategies:

- Limiting the amount of the value stored or providing large traceability of important transactions or large number of contracts.[2]
- Providing conditions on internet banking contracts with customers reminding them that the bank is not responsible for their fraud or money laundering and such crimes may be traceable for unlimited times.

---

[1]-http://swiss-bank-accounts.com/e/banking/secrecy/money.laundering. definition.html

[2]-Froomkin, A. Michael, Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases, University of Pittsburgh Journal of Law and Commerce, Vol. 15, 1996. p. 403.

- Improving authentication methods and procedures and a recording system to protect against the theft of confidential information,[1] tax evasion and money laundering.
- Increasing suspicious activities monitoring and employing additional identity verification control.[2]
- If crimes are detected in connection with customers' accounts, the bank should report the details of crime to the police and all its customers and take reasonable steps for preventing similar crimes in future.

6- Consumer Protection

The concept of "consumer" is defined in Article 2 of IECA. According to this paragraph, consumer is "Any person acting for any purpose other than business or professional occupation". The Act has comprehensive protecting provisions for consumers in Articles 33-49. Of course, Article 49 stipulates that "Consumer's rights when dealing with electronic payment systems are subject to rules and regulations which have been or will be ratified by the relevant legislative authorities". Thus this is an unsaid matter in Iranian positive law that the consumer in electronic payments must be protected by statutes.

In the meantime, the rise of consumer trade in internet presents a factual pattern never seen before.[3] The internationality of these transactions has offered the fact of thinking to general coverage for cross

[1]- Gillett, Mark T; Obrea O Poindexter; M Sean Ruff, Developments in Cyberbanking, The Business Lawyer, May 2004. p. 1336.

[2] - Ibid, p. 1337.

[3]- Davis, Lars, The Internet and the Elephant, International Business Lawyer, April 1996.

border consumers. For determining the limits of consumer protection, it is important to realize applicable law on consumer contracts. For this, some of the traditional connecting factors may be used, such as the place of contracting or performance and these factors can become fortuitous in an online environment.[1]

Basically, in internet banking, these factors are not applicable because in standard form of contract which is provided and downloadable from the website of a bank, this clause is often included that the contract between bank and any customer is subject to applicable law determined by the bank. Of course, this determination is facilitating fact for banks which is securing them to confront with different laws from different systems. Notwithstanding, the applicable law for a bank-consumer contract can not be interpreted so far as obstacle depriving consumer from certain protective provisions of his country (the place in which he has domiciled).

In spite of purchase or supply contracts, the concept and scope of consumer protection are practically limited in internet banking. Thus "the right to withdraw", which is recognized for the consumer by Article 37 of IECA, will not be established in internet banking contracts because the standard form of contract between a bank and a consumer is stipulating this clause and as another reason, due to preserving third party's rights, e.g. seller of goods for consumer, there is no justification for recognizing the right of withdraw for consumer in payment contracts.

---

[1]- Schu, R, The applicable Law to Consumer Contracts Made over the Internet: Consumer Protection Through Private International Law? International Journal of Law and Information Technology 5 (2), 1997. p. 194.

7- Supervision and Monetary Policy in Internet Banking

Many countries have revamped their regulatory systems to establish a single regulator for all three sectors, i.e. traditional financial sectors,[1] banking securities and insurance. In summery, financial services (banking and insurance) are subject to a single organization. But in other countries, including Iran, have separate regime for supervision for banking and insurance, i.e. The Central Bank of The Islamic Republic of Iran for banking affairs and The Central Insurance of Iran for supervising insurance services and companies.

Another problem is about the combination or separation of monetary policy and bank supervision. Should the central bank undertake both the policy and supervision in internet banking? In Iran the roles are recognized for central bank of Iran. Therefore there seems to be no difference between traditional and new methods of banking from the view of supervision and monetary policy.

The role of central bank as supervisor of the payment system may extend to cover new areas; for example through consulting market operators, promulgating rules for market operators to certain behaviors and to offer directly certain services.[2] "The benefits of combination do not reset solely on what happens in successful times. Combining bank supervision and monetary policy allows central banks to consider the

---

[1]- Schooner, Heidi Mandanis, Central Banks' Role in Bank Supervision in the United States and United Kingdom, Brooklyn International Law Journal, Vol. 28, 2002 – 2003. p. 411.

[2]- Cipparone, Mauro, The Role of the Central Bank in the Growing Industry of Internet Payments, Journal of Internet Banking and Commerce, Vol. 1, No. 5, September 1996.

border consequences of supervision".[1] Thus concerning internet banking in Iran, from legal aspect, it seems that a single organization should be undertaken both monetary policy and bank supervision. The best choice for this combination is The Central Bank of Iran which can be considered as a bridge between traditional and modern banking.

8- Conclusion

In the ocean of information, exchange of financial information should not be considered as strangers' ramble in the desert. Because, on one hand, not all of internet banking transactions has a new nature from the view of law so there is no need to elude further from new chances opened for economic development. On the other hand, any new method can have linkage with traditional bases of law. Therefore, we can justify modern banking methods of transaction by necessities deriving from information technology revolution.

Of course, the new system of banking should be designed and developed within constrains and norms of the legal requirements. Hence, internet banking should not be supposed as an exceptional structure that is able to break legal rules and draw disparate regime. Our country, for collaboration with other systems and for keeping step with the new world, needs a comprehensive Act on different aspects of internet banking. Use of new technologies in banking is considered as innovative and competitive factor for financial sectors. Thus, these means of communication should not be denied or rejected only by reasoning on it's primarily damages to national economy. The future belongs to provident men and the world, in the way of development, will not wait to anyone.

---

[1]- Haubrich, Joseph G, Combining Bank Supervision and Monetary Policy, Economic Commentary, Federal Reserve Bank of Cleveland, November 1996. At: www.clevelandfed.org/research/Commentary/1996/1196.htm#int

Reference

1- Arora, Anu. (1999). *Electronic Banking and the Law*. Secend Edition. London: Banking Technology. Inc.

2- Barnes, Richard, L. (2005). Rediscovering Subjectivity in Contracts: Adhesion and Unconscionability. *Louisiana Law Review*, 66. (1).

3- Berger, Vivian. (1982). Criminal Liability of Bank Directors. *American Journal of Comparative Law*, 10.

4- Brousseau, Eric & Jean-Michel Glachant (Ed.). (2002). *The Economics of Contracts: Theories and Applications*. Cambridge: Cambridge University Press.

5- Burgess, Andrew. (1986). Consumer Adhesion Contracts and Unfair Terms: A Critique of Current Theory and a Suggestion. *Anglo-American Law Review*, 15.

6- Cipparone, Mauro. (1996). The Role of the Central Bank in the Growing Industry of Internet Payments. *Journal of Internet Banking and Commerce*, 1.(5).

7- Delta, George, B. (2000). State Taxation of the Internet: A Review of Some Issues. *Willamette Journal of International Law & Dispute Resolution*, 7.

8- Dickie, John. (1998). When and Where are Electronic Contracts Concluded. *Northern Ireland Legal Quarterly*, 6.

9- Goode, R. M. (1985). *E-Banking, the Legal Implications*. London: The Institute of Bankers, University of London.

10- Goodman, Marc, D. (1997). Why the Police Don't Care about Computer Crime. *Harvard Journal of Law & Technolgy*, 10 (3).

11- Gutwirth, Serge & Joris, Tony. (1991).Electronic Funds Transfer and the Consumer: The "Soft Law" Approach in the European Community and Australia**.** *International and Comparative Law Quarterly*, 40 (2).

12- Hill, Jennifer, E. (2003). The Future of Electronic Contracts in International Sales: Gaps and Natural Remedies under the United Nations Convention on Contracts for the International Sale of Goods. *Northwestern Journal of Technology and Intellectual Property*, 2 (1).

13- Robins, Mark, D. (2003). Evidence at the Electronic Frontier: Introducing E-Mail at the Trial in Commercial Litigation. *Rutgers Computer & Technology Law Journal*, 29.

14- Rogers, James, S. (2005). *The New Old Law of Electronic Money*. *Boston College Law School Faculty Papers*, 39, March 3.

15- United States Department of the Treasury Conference. (1996).*Toward Electronic Money and Banking: The Role of Government*, September 19-20. Washington, D.C: United States Department of Treasury.