IOSR Journal of Economics and Finance (IOSR-JEF)
e-ISSN: 2321-5933, p-ISSN: 2321-5925.Volume 8, Issue 1 Ver. III (Jan-Feb. 2017), PP 32-39
www.iosrjournals.org

Contractual Liabilities in Internet Banking Contracts

Nariman Fakheri [1], Zahir Jafarniya [2], Seyed Gani Nazari [3]
[1.] *Assistant in PAYAME NOOR University, IRAN*
[2.] *Master of International Law, IRAN*
[3.] *Master of Criminal Law and Criminology, IRAN*

Abstract: *The modern world deals with great changes on communication of information and development of new technologies of communication and information, making it inevitable to apply new management, economic, political, and legal methods and strategies. The new information and communication that is the basis of management in the modern world requires proper mechanisms and infrastructures in order to make the development of business and good environment for entrepreneur possible. One of the most important infrastructures is internet banking. Arising any issue, whether political, social, economic, or cultural, has consequences associated with different internal or international outcomes, regardless of their positive or negative results. Since financial issues have been always the most challenging issues in human societies, internet banking is dealt with economic issues in a different and new way and hence, it may include regulations to meet, internally or internationally, the legal needs of clients and custodians and contribute to developing this technology further. Global central bank thinking and a uniform treaty for internet banking with strategic rules and regulations to resolve the financial disputes arising from internet banking is an instruction for pragmatists in reaching a global uniform procedure, which is considered as the most important outcome of modern communication, i.e. internet banking. Drafting and adoption of the International Convention on internet banking under considerations of the United Nations Commission on International Trade Law through instructions and procedures of the central bank providing two conditions of goodwill and safety is an introduction for the realization of internet banking, which needs the contribution and cooperation of all countries including Iran. Internet banking may be misused and have harmful consequences for economy as much as it can contribute to develop economic, financial and banking activities. Aiming at improving internet banking and treating against violators and maintaining the clients' values, legal rules, either internal or international, are to maintain the clients' rights on the one hand and contribute to strengthening the foundations of this new economic technology on the other hand. In this context, this paper aims at study the legal aspects of internet banking in contexts of internal and international laws and explores the related rules with this technology briefly.*

Keywords: *Electronic banking, Internet banking, Competent court in internet banking*

I. Definitions and Concepts

1.1. Electronic banking

"Providing banking services through a publically accessible computer network (Internet or Intranet) that is highly secured" or" providing customers access to banking services by secure intermediaries and without physical presence". The transformation of a banking system and turning to electronic services depends on the state economic policies and providing legal and administrative frameworks as well as developing information and communication technology. Obviously, changes in any country depend on the culture of that country and the changes in internet banking is not an exception. Computer software and software systems are used in electronic banking.

Generally, electronic-banking is banking operations through centralized computer systems, networks with widespread accessibility, and the lack of time and space constraints and information security (using credit cards, ATMs, global union services, interbank financial telecommunications, satellite communication lines, banking at home, software, and remote banking are all services by electronic banking). It is said that electronic banking is using electronic devices in offering banking services, which is in turn classified under electronic funding. Providing a communication network between the clients and banks at internal or international levels is the starting point for electronic banking.

1.2. Internet banking

Internet banking is a part of electronic banking; indeed, it deals with banking operations by World Wide Web. It includes providing services to clients through Internet so that they can organize or change their accounts or invest and do other operations.

1.2.1. Digital (electronic) signature

It is one of the best secure practice in internet banking, which is as old as electronic business and is sometimes in a general sense referred to as electronic signature and is the result of cryptography (the science that solve the codes of a text by mathematics, software and hardware methods and the receptor can use the same algorithm to encode them). Any sign is attached or connected logically to the data of that message, which is used for identifying the signer of the "data of message".

1.2.2. Internet Service Provider (ISP)

Internet is a global network of communication networks, has become a powerful communication tool in internal, regional, and international affairs. In users' views, ISP serves as a bridge to connect to the Internet. In this context, users can access to what is accessible and allowable in the World Wide Web, share their information and send or receive messages in different forms. ISP is efficient in internet banking. Connection with internet is canceled without ISP since it serves as a bridge between the content and the receiver of information; in fact, it is considered as a network interface.

1.3. Contracts of Internet Banking

Internet banking is a structure based on agreement and contract. Agreement between the parties provides the chance to use analyses based on the laws in contracts. Internet banking requires detailed contracts, showing the rights, interests, and obligations of each party as much as possible and prevent the possible disputes. The internet banking contracts are specifically between the bank and user; in these contracts, the client is required to fill an online form and write his/her ID number, account number, and password.

The obligations for the parties include rights and liabilities whose consequences and executive enforcement are separately specified. The bank agrees to keep the personal information of client confidential and accept the consequences for the failure of the obligation to provide banking services stipulated in the contract. The client agrees to keep the information of good will confidential, and confirm the disclosure or lack of ID number to the bank. Such contract is a prewritten form (in a standard from for the branches of that bank) and accessible in the Internet. The contract is the starting point for the relation between parties in internet banking.

1.4. Internet banking contract

Contracting with the offer and acceptance is the general rule of all contracts. The first proposal by any party, which is associated with intention is called offer and if the other party accepts that unconditionally, it changes to a binding contract in the relation between the parties. According to the general rules of the contract law, any contract in principle is concluded after preliminary and final negotiations on the deal and essential and non-essential conditions. Internet banking contracts, like the other contracts, must have the basic conditions of transaction validity and the special conditions of banking contracts.

"The principle of requirement to offer" that is properly considered in some countries makes the party who withdraw his offer with no reason accountable for compensate the losses of the other party. If it is proved that the parties have agreed, offer cannot be withdrew and any action would be regarded as "violation of the contract". It is assumed in internet banking contracts, like the other contracts, that there is no additional condition for agreement and acceptance requires contracting; providing the banking services, in its special terms, requires accepting the offer by bank through formalities. Any change in the required conditions set forth in offer by the bank if is not agreed by the client violates the peremptory provisions of the contract and is somehow regarded as the imposition of the conditions to the client. This problem can be rarely seen in internet banking contracts since the bank (as the party of acceptance) sets the form and this is the client who agrees with the conditions.

1.4.1. Contractual liabilities in internet banking contracts

We discuss about the contractual liabilities when failure in fulfilment of obligations in contract cancels the validity of that. The liabilities of bank and client, in contractual liabilities of internet banking, is not only of consideration, but also the liabilities of those involved in the contract. According to the contractual liabilities, anyone can refer to one with whom s/he agreed; no third party can be claimant but in some cases a third party can refer as "beneficiary".

1.4.2. IPS contractual liabilities in internet banking

IPS services are provided in the form of an agreement containing the specifications of the parties. In addition to the precision of the contract, some other liabilities may be imposed to the IPS of internet bank due to an implied term or online services. According to the contract, IPS undertakes providing services, updating communication technology, communicating securely and reporting any risk, technical violations by those who

access the system and preventing financial crimes in cyberspace in which the banking transactions occur. IPSs are mostly under upper level management of special organizations. In England law, the cases about the liabilities of IPS or people with comparable profession are related to personal and confidential data.
Generally, it can be inferred from the criteria in these cases, e.g. Totaliz and Godfrey, that IPS is required to the standard precautions to avoid disclosure of secrets and electronic information belonging to others, if it had just the mediator role, and the court can sentence the IPS to compensate all material and intellectual property losses by considering the condition if IPS failed in keeping the data confidential or making disruption in the relation between the parties.

The accountability of Rasa for the use of any password for the exchange of information, without obtaining the consent of the relevant authorities and registering the characteristics, algorithm and the key for the password and recording the applicant's information in the Secretariat of the Supreme Council of Information (or another institution offered by the Secretariat) has been recognized. Using password for exchanging information by Rasa aims at avoiding the control of the nature of the exchanged information by other individuals and organizations. Since any password has an algorithm used for decoding that, control of the exchanged information in Rasa networks by authorities needs obtaining the approval of the relevant authorities and registering the characteristics, algorithm, and the key of that password as well as the characteristics of the applicant in the Secretariat of the Supreme Council of Information or the institution offered by the Secretariat. It should be noted that using a password is required to keep the information confidential and secure; information like bank accounts. Failure in this matter can be result in trade sanctions and, if it harms the others, civil liabilities. This liability is the consequence of wastage.

1.4.3. Consumer liabilities for unauthorized transfers

If the client gives his debit card and personal ID number to one of his friends or relatives and that person withdraws money from that account without the owner's consent or overdraw money, the holder of the account has to compensate the losses. Similarly, if the client allows someone to withdraw money from his account and that person falsely claim for theft, the holder of that account has to compensate the losses. However, in this case, the client would be accountable if the financial institution could prove that the fraudulent withdraw had been under the holder's consent. Otherwise, the client would not be accountable.

In cases where the electronic funds transfer is unauthorized, the electronic transfer law considers the three fundamental credits for maximum liability. According to Article 205-6, if the client refrains from reporting the unauthorized transfer within 60 days by the periodical declaration of financial institution for detailed reports of electronic funds transfer, he is fully accountable. On the contrary, if the client reports missing the credit card to the financial institution, his liability will reduce to minimum funds withdrawn fraudulently from his account, i.e. 50 dollars or amount withdrawn from his account. Failure to report theft or loss of the credit card by the client or any other means to access to his account lead to his liability to all the amount that:

a) The actual loss is more than 50$ and has been within two business days.
b) The actual loss (the amount withdrew fraudulently) occurred within two business days would not be over 500 dollars in any case of theft or losing.

In any other fraudulent uses, the client's liability would be 50 dollars. Under *the good will on loan* act, the same will be for losing credit card. According to the interpretations by Federal Reserve Board, 50 dollars should be paid as compensation for loss even if the transfers from the lost account are many. This analysis conforms to the good will on loan act based on which the client's liabilities on lost credit and debit cards, regardless the numbers of transfers, are some dollars. It should be noted that these amounts in credit transfer rule are only suggestions (supplementary rules) and the contract between the parties can violate that.

1.4.4. The financial institution's accountability in unauthorized transfers

The financial institutions will have civil liabilities in cases where they are required to transfer funds at the client's request and neglect it despite the possibility, due to fault or negligence, or where the client asked for stopping the transfer operation but they decline it. In cases where the institution cannot stop the transfer operation due to unintentional and inevitable error, the demanded compensation would be as much as the actual loss. The same client can demand the actual compensation from anyone involved including the financial institution that made a mistake due to violating the electronic transmission of credit law. In electronic transmission of credit law, like good will on loan act, a determined amount, according to the peremptory law (Article 1693 (m) (a)), is predicted to be paid for compensating the loss caused by violation of the provisions of law. Therefore, if the client can only prove the technical violation such as failure of the financial institution to submit the declaration within the prescribed period, s/he is entitled to compensation for 100 dollars by the financial institution even if there is no loss for him/her. In cases where the client demands the actual loss form the financial institution, he can demand honorarium and other expenses.

The Electronic transmission of credit law has predicted the following defenses against civil liabilities for financial institutions:

1. Happening an unexpected event caused by an error with no bad intention though conventional solutions are predicted for preventing happening such events.
2. Trust and good will about the regulation, instruction, or interpretation provided by the Federal Reserve Board; the institution can use it for defense in case of proving its good will.

There are also other alternative arbitrary solutions for avoiding the legal liabilities; for example, the financial institution can re-open the client's account before or after the liability lawsuit by the client and compensate the actual or estimated loss. This case can be found in Article 1693 electronic transmission of credit.

1.4.5. Criminal liability in unauthorized transfer

Criminal liability is for anyone who provides incorrect or imprecise information or his action is against the provisions of the electronic transmission of credit law. This liability is imposed on not only the client who falsely claimed that the credit/debit card has been stolen, but on the financial institution that violates the technical standards provided by the electronic transmission of credit law. This law has stipulated the punishment for unauthorized use of debit document, according to Article 1693 (n) (b). Any conspiracy for collusion, dishonesties, falsification, forgery, loss, theft, or making a fake debit document can incur penalty for ten thousand dollars or more, more than ten year's imprisonment or both. Criminal guarantees like these are important since it was impossible to prosecute some crimes such as forging debit card before passing the electronic transmission of credit law. Such serious punishments indicate the legislator's in protecting the financial, banking, and economic systems of the country.

In Iranian law, the tone of Penal Code articles on corruption, and economic, monetary, and banking crimes, including Articles 518-522, Paragraph 5 Article 525, and Article 526 is in a way that it is not possible to infer the punishment for crimes against electronic payments, and since any argument about the "spirit of the law" or extended interpretation of the materials on crimes is contrary to legal principle of the crimes and punishment and the need for a strict interpretation is in favor of the defendant, it is impossible to apply the Islamic Penal Code articles criminalization of electronic crimes. However, in accordance with Article 6 Computer Crimes Act: "anyone committed the unauthorized actions is a forger and will be imprisoned one to 5 years or punished to pay 20 million Rials to 100 million Rials, or both:

a) Changing or creating reliable data or creating or adding false data to reliable ones.
b) Changing data or signals of memory cards or signals can be processed in computer or telecommunication systems or chips or creating or adding false data or signals to them.

Article 518 Islamic Penal Code and Articles 1 the law of intensification of punishment for the perpetrators of corruption, embezzlement, and fraud (passed by the Islamic Consultative Assembly in 1985 and approved by the Expediency Council in 1988) can reveal the legislator's general approach to criminalization of financial and economic crimes- particularly in the monetary and banking violations. According to Article 518 Islamic Penal Code, "anyone who makes the things like gold or silver domestic or foreign coins such as gold coins, coins of the previous governments in Iran, lira and other currencies that are used for transactions or import them into the country deliberately and trade them will be sentenced 1-10 years imprisonment.

There are two important points in this Article: first, the material is not limited to coin, money, or currency and can be included other currencies or new credits though such extended interpretation violates the Constitution and criminal law. Second, the serious punishment by the legislator indicated the importance and significance of the monetary and financial issues since they affect internal and external securities. In this regard, the electronic payment types, as extended to cards, cannot be neglected. The existing regulations should be legalized without any attempt to make limitations for them.

Other Articles, as well as the one mentioned above, may be considered by the domestic judge. According to Article 1 the law of intensification of punishment for the perpetrators of corruption, embezzlement, and fraud, "anyone deceives people into thinking there are false companies, businesses, factories, institutions, or false properties and authorities and makes unrealistic hopes, and terrors by unreal events or pick a forged name or title, and earn money, funds, properties, documents, drafts, or bills or recoupment accounts by one of these ways or any other false ways and seize others' properties is swindler and has to return the property to the holder and is sentenced to 1 to 7 years of imprisonment and pay fine as much as the financial scam. In the cases where the perpetrator is an employee in state (or state-controlled) corporations, state agencies, state-owned companies, councils, municipalities, or revolutionary institutions and in general three powers as well as an officer in the Armed Forces and is assigned to public service, or in case where the offense has taken place by using propaganda through mass media such as radio, television, newspapers, and magazines or public talks, or printed or handwritten publication, or in the cases where the perpetrator is an employee in government, state institutions and companies, or state-controlled companies, municipalities, or revolutionary institutions, who serves the public, the offender has to return the property to the holder and will be

sentenced to 2-10 years of imprisonment and life suspension of service and pay fine as equivalent as he received by fraud".

Moreover, it seems that Article 67 Electronic Commerce Act is more clarified and up to date in terms of considering the punishment for criminal acts in cyberspace. According to this Article, "anyone deceives others, in electronic transactions, by misusing or unauthorized use (of messages), applications and computer systems, telecommunication equipment, and committing acts such as logging in, fading or stopping (messages), making malfunctions in computer program or system, or cause errors in automated processing systems and, by doing so, earns money, properties, or financial assets and seize others' properties is criminal and has to return the properties to the holder and will be sentenced to 1-3 years of imprisonment and pay fine as equivalent as he earned by fraud". According to the note of this Article, "starting this offense is regarded as crime and is punishable by the minimum punishment described in this Article". The punishment for such crimes is serious, indicating the importance of electronic commerce issues and financial and legal matters as well as rights, and responsibilities of those involved, from the legislator's perspective.

Finally, in accordance with Article 11 Computer Crimes Act, "anybody commits the actions described in Articles (8), (9), and (10) in this Act against computer and telecommunication systems use for providing essential public services such as health, water, electricity, gas, telecommunication, transportation, and banking, and intents to endanger the public security and peace will be sentenced to 1-10 years of imprisonment". Different laws on crimes and punishment and lack of consideration to electronic payments in these laws indicate that lawsuits on electronic payments only will lead the Iranian judge to confusion since he has to consider many similar cases criminalized extensively on these acts and have no specific relation to electronic payments. Particularly, according to Article 49 Electronic Commerce Act, "consumer rights when using electronic payment instruments are under regulations passed or will be passed by the relevant authorities". Since the consumer rights are not clarified in this Article, it can cover criminal supports as well. Therefore, this matter needs to be considered and clarified, helping the judge to avoid his preferences in the judgement and determining the exact punishment and the conditions of the electronic payment crimes.

1.5. The effect of good will on evasion of responsibilities on electronic payments

In this case, the Iranian law- like other issues on electronic payment laws- has nothing to represent. However, according to what has been said about the American law and analyses of regulations in contracts in Iran, it can be inferred that good will can be helpful and effective on evasion of responsibilities in the cases where electronic payment is problematic. In American law, the provisions of Electronic Transmission of Credit law are similar with those stipulated in Providing Fair Debt law and both are documented in the decision of court in Bingham case. What is common in these three cases is that the defendant must prove that the offense has not been intentional and resulted from an "error with good will" to be exempt from responsibilities. Moreover, the defendant must prove that he had done conventional measures to avoid such errors.

The same is true in Good Will on Loan Act in which there is a narrow sense of exemption from responsibilities. In Paragraph 4-402 of Commercial Uniformity Act, there is no expression imposing commitment on doing conventional acts for prevention to the bank and courts have not, at least expressively, determined such commitments. In this regard, any interpretation of error with good will has to be narrowly done and be limited to unintentional errors. This conforms to the legal principles as well since knowledge about error negates good will, indicating that the person neglected this matter though it had been possible to avoid such an error conventionally. Article 227 Civil Law in Iran states that "the offender who fails to fulfill his responsibilities will be punished to pay compensation when he cannot prove that this failure has been due to an external cause unrelated to him". According to Article 229 Civil Law, "if the committed person fails to fulfill his responsibilities due to an event out of his authorities, he will not be subject to pay compensation".

II. Legal-security aspects of internet banking

2.1. Security and crimes against internet banking (in context of internal and international laws)

Boarding internet banking services is one of the major advantages but one of reasons for reducing security in this type of banking. One of the important issues with which the financial institutions face when providing monetary and banking services is security. There should be specified some factors through which security of the system will be guaranteed.

2.2. Internet banking security by encryption, digital (electronic) signature

Digital signature is one of the safest ways to guarantee security in internet banking. At first glance, electronic signature is the same as handwritten signature with similar legal consequences. Through digital signature or cryptography in general, one may prove non-falsification of the message, the identity of the signer, and the sender's content verification. The advantage of digital encryption is that if the singer loses the private key control, e.g. forgets that, there is no way to frog what had been created before.

The electronic signature in general sense is classified in two forms: first, any signature or sign formed electronically; typing the full name of signer, a scanned picture of the signer, handwritten signature of the holder in an electronic document or biological ID (fingerprint, symmetrical picture) or face are regarded as electronic signature. Digital signature is expected to follow the same goals considered for signature in real life. A perfect digital signature guarantees verification of the sender's identity; the sender cannot deny the signed message and the receiver cannot forget it, without being discovered. Article 10 Electronic Commerce Act states "safe electronic signature" under four conditions:

a) It is unique for the signer.
b) It shows the identity of the sender's "message".
c) It is made by the signer or under his/her exclusive will.
d) It should be connected to a "message" in a way that any change in that "message" is discoverable.

2.3. Probative value of electronic signature

The claimant has to prove the safety and security in signature. The demonstrator has a serious responsibility that can be helped out by standard versions provide by valid organizations such as international standardization organizations.

2.4. Fraud in internet banking

The most sophisticated financial crime is internet fraud by which the professional criminal can steal others' properties by combining several offenses such as making a false password, unauthorized access, computer forgery, and identity theft. Misuse has a general sense in internet banking and its examples that result in seizure of properties may not be classified under the offenses of fraud. Cheating in internet banking may be happened by unauthorized entries into bank system or by one of the clients (or his/her assistance) and a professional expert.

III. Internal And International Cooperation For Preventing And Fighting Against Internet Banking Crimes

The cooperation of local organizations as well as governments at international level is of great importance to decrease such crimes. Crimes may be happened at transnational level and by those unknown for bank, and hence, prosecution of such criminals would be possible only by cooperation of countries.

There have been predicted global standards to prevent committing crimes in internet banking and banks are required to provide training programs for their clients in internet bases of the bank and remind them the problems of security in internet banking. In Swiss law, one of the security sources in banks is international treaties of this country. Security in banking is a liability in the contract between the parties and violation can result in contractual liabilities. Membership in regional, international, bilateral or multilateral treaties is one of the ways to enhance security that could have been paid great attention in the European Union.

Privacy in itself is a unique basis to interpret punishment in internet banking; that is, bank, clients, and ISP have certain privacies and any breaking such boundaries are subject to liabilities.

The most important function of international cooperation in internet banking laws in the future is uniformity in regulation of this type of banking, which has been achieved in some criminal aspects of banking like money laundering. Uniformity in international laws regarding internet banking in contractual aspects and civil liability is not too far-fetched.

IV. Conclusion

Internet banking is part of development in banking and the outcome of electronic banks and other ideas including generalization of economy. Indeed, internet banking is an advanced from of electronic banking can go beyond borders and challenges countries with important issues like protecting the national economy at macro level. Though following the same legal rules on different aspects at internal or international levels, it may depend on special analyses of internal or transnational rules in terms of the issue. At international level, internet banking has opened new horizons for rules that cannot be analyzed by relying on rules on private rights. When there are legal limitations and penal enforcement against transnational banking, the global network of communication cannot be excused to escape from law. At internal level, it can be claimed that electronic banking regulations are enforceable, except on security issues that need to be discussed in details, and only big transactions should be of greater caution. The problems such as the location of contracting, the place of implementing commitments, terms for claiming compensation can be resolved by making the contractual relations clear, minimizing the disputes in the future.

A question here arises how the Iran's future approach towards the important issue of internet banking will be drawn, whose "international" version is of great importance. Iran's future approach towards international internet banking is too economic since this issue is very important. In fact, governments are largely coordinated

in terms of rules and regulations and the global village is increasingly shrinking and internet banks offer banking services more than ever through standard contracts in which customers' freedom and right to choose are emphasized. Therefore, regional currency rather than national currency has been suggested. Changes in communication space has been influenced by modern communication means, and has challenged organizations and people, before governments, to do business in the new space. All changes require agreements between governments at international level and passing law at internal level. These agreements should be under Constitution if their political-economic procedures are legitimized.

V. Practical and executive strategies

In contracts between internet banking and client, the negotiations that are effective and are regarded as a way to respect the clients should be possible; the court cannot interpret the contract arbitrarily or broadly. The additional contract is required to be interpreted in favor of a third party who is not involved in it, due to the influence and control of the contractor.

The practical procedure has been developed recently on electronic contracts between bank and clients is that the internet bank stipulates in the contract that the location of contract is bank and the contract comes into effect when the agreements are done and the deposit is paid to the client.

Despite growing interest in internet banking, ambiguity in the nature or lack of information have made doubts in dealing with this type of banking, especially those in middle or lower classes of society; they are afraid of unsafety or disclosure of their financial accounts and may not believe in internet bank as a good way to achieve their goals. "Preventive measures", for some, albeit with financial or time costs, are rigid beliefs and what can change such traditional beliefs to accept internet banking is clarification of different aspects of internet banking. Since bank is associated with clients, this matter is of great importance.

Since the contracting human party cannot be included under technical regulations such as "encryption", the rules might be violated; therefore, banks should consider measures to warn the clients on the one hand, and to guarantee their security on the other hand. If any disagreement occurs between bank and client, the contract and the provisions are the criteria for action. Because, the true and common intentions of the parties should be considered to evaluate the form and provisions of the contract and should not be bound to terms or titles used mistakenly by the parties to keep secret the true nature of the contract. On the crimes against internet banking, it should be noted that prevention or prosecution requires organizations, institutions, internal legal and real persons and governments at international levels; realizing this matter, the required executive measures, according to the future penalty for computer crimes, should be considered in the country.

Those parts of crimes against internet banking, which have not been subject to penalty due to lack of history in the current law, should be criminalized after considering the social and economic consequences. The most important function of international cooperation for the future internet banking is uniformity in regulations and rules on this issue. This uniformity has been achieved to some extent in criminal aspects of internet banking, including money laundering. Uniformity in international regulations on internet banking in different aspects of contracts and civil liabilities is not far-fetched. Particularly, since the issues such as management, safety strategies, information exchange, and multilateral business contracts are common interests in countries, unlike issues like money laundering, which are political at macro levels. Therefore, international uniformity in such common interests can legalize them as well.

As the governments' failure to cite the restrictive internal regulations on international trade can be accepted through the necessity of good will in international relations, everyone should do his best to use the expertise and precautions to provide the national interests while agreeing with international internet banking infrastructure development contracts. Failure in choosing the dominant rule in the relation between bank and client requires the Iranian court to follow the Iranian Law, except for the cases in which the law is not related or has predicted no special regulation to solve that problem.

On internet banking, the principle is that the court where the crime has occurred and the court where the domicile of the claimant is have authorities to jurisdiction for crimes and civil issues, respectively. This principle should be considered at both internal and international levels to recognize the city (jurisdiction) and the country whose court have the authorities for jurisdiction.

The dominant rule in non-contractual liabilities in internet banking has to be a related and predictable one. Achieving this goal, the recognition criterion may be changed from the location of loss to a rule with more relativity in order to protect the rights of consumer who used the services of online internet bank. Realizing the true policy-making role of the Central Bank on internet banking, two functions should be considered for this institution: supervision of all banking operations and regulating the rules of currency transactions.

Iran follows the rules of Islamic banking, and it should be considered that operations in internet banking require protection of regulations such as "interest-free banking regulation" and development in internet operations should not disrupt the implementation of these regulations. The internet banking operations have to be in the form of public joint stock company under monetary and banking rules of Iran though the banks can

have the license for such operations. An unbiased supervisor, on issues of internet banking, should predict the cautions to prevent crimes and protect consumer rights; it seems that, except for crimes and violations relevant to law enforcement and judicial institutions, the Central Bank is an appropriate supervisor.

On internet banking in Iran, like in other banks in the world, the unity between the supervisor (e.g. Central bank) and regulator should be accepted. Since rapid exchange of information in banking operations allows the Central bank to notify the other involved banks about problems and challenges in internet banking, especially in the early years of this form of banking establishment. The internet banking operations have to be in the form of public joint stock company under monetary and banking rules of Iran though the banks can have the license for such operations. Two factors, i.e. skill and precaution, as the main factors in internet banking should not be ignored. In fact, internet banking would be distinct from its general term if it predicts skill and precautions (in conventional forms of civil liabilities).

References

[1]. Abbasinejad H. Mehrnosh M. (2010). Electronic banking. Samt Publications. Tehran.
[2]. Abdollahi M. Shahbaziniya M. (2010). Reliable information systems in e-commerce law. Journal of Legal Research. 16.
[3]. Allahyarifard M. (2004). E-banking services and the administrative needs of its comparative operating expenses, various banking services. Monetary and Banking Research Institute. Tehran.
[4]. Avovoanu, Electronic banking and the Law‹London, 1999, PP. 212-219.
[5]. Delta‹George‹Willamette Journal of Internatinal Law and Dispute Respute Resolution Vol.7‹2000
[6]. Elsan M, Yamchi D. (2002). Computer nature and legal aspects of digital signatures. Quarterly Journal of Judicial Law Views, 30.
[7]. Elsan M. (2007). The digital signature on documents in an electronic form. Legal Monthly Association of notaries. 55.
[8]. Elsan M. (2014). Low of Internet Banking. Monetary and Banking Research Institute. Tehran.
[9]. Elsan M. (2015). Cyberspace Law. 1 ed. Shahre Danesh Publications. Tehran.
[10]. GordomLesliea‹Banking on Faith ‹American Bar Association Journal‹Vol.91‹2005.
[11]. Gosnell C. (1988) Miami Law Review. Canadian Business Law Journal, 29.
[12]. GROUP Oftem/ReportonConsolidationin the Financial sertor 2007. Sakabdeen and etal‹op.Cit‹p.304.
[13]. Haubrich by Joseph G(1996).combining Bank supervision and Monetary Policy, WWW.Clevelandfead.org. UNCTAD E-Commerce and Development Repert 2001 p .168.
[14]. Hoenig‹thomasm‹Federal Reserve Bank of Kansas city Economic Review‹1996. O,Driscoll‹Gerald‹Catogornal‹Vol.7 No.3‹1988.P.661-675.
[15]. Katozyan N. (2014). General rules of contract. Corporation Publications. Tehran.
[16]. Luftman, Douglas B, Defamation Liability for online services: The Sky is not Falling, George Washington Law Review, Vol. 65 (6), 1997. p. 1096.
[17]. Magnin, Cedric J. (2001) "The Telebanking Contract In Swiss law," ILSA Journal of International & Comparative Law: Vol. 8 : Iss. 1 , Article 3.
[18]. Marcucci‹Jacgueline‹Nova law Review‹Vol.23‹1999.p.755 .
[19]. Mehdi Khosrow-Pour. Encyclopedia of Information Science and Technology. USA. 2008. P. 432.
[20]. Mokey‹Ul rich and Hans-Jurgen‹Thenorth American Journal of economics and Finance‹Vol.7(2)‹1996.
[21]. Nikbakht HR. (2004). Issues raised in the law governing the contract. Journal of Legal Studies. 39.
[22]. Schooner‹Heidi Mandanis‹Brooklyn Internatinal Law Journal‹Vol.28‹2002-2003.
[23]. Sean M. O'Connor. The De Minimis Exemption of Stored Value Cards from Regulation E: An Invitation to Fraud.Richmond jounal of law and Technology. Vol V‹ISSUE 2‹Winter1998.
[24]. Seyed Javadin, R. Saghatchi, M. (2006). Electronic banking and evolution in Iran. Tadbir Monthly. 170.