

E-BANKING AND OTHER FINANCIAL SERVICES: REGULATORY DEVELOPMENTS IN SELECTED ARAB COUNTRIES

Mohamed Y. Alem
Alem & Associates
Beirut - Lebanon

I. Introduction

During the last twenty years the world has witnessed a drastic change onto the way business is conducted, services are rendered, products are sold and communications handled. Indeed, the technology revolution has had a profound and irreversible impact on the way the world is moving and interacting whereby the new technologies provided for cheaper, easier and faster solutions to the traditional way of living.

Nowadays, most people are familiar with new expressions such as e-services, e-commerce, e-government, B to B (Business to Business) B to C (Business to Consumer), etc... I would recall that only four or five years ago the mere use of one of these expressions would generate a very obvious panic for lawmakers, government entities and both judges and lawyers as well.

The question was then basically revolving around how to accommodate such developments in already existing laws and how to regulate this new world that started to become as important as the real world from a concrete and clear legal perspective.

One cannot say that all new issues are now resolved and that solutions are today available on hand, however, one should recognize the tremendous efforts and profound legal developments that started to affect the new ways of conducting business through the use of new technologies.

Though such technologies have affected a very substantial and wide array of business activities, the legal challenges displayed by the introduction and use of new technological means to both, banking and financial services might be one of the most defying tasks confronting the international business and legal communities which has already required substantial amounts of discussions, debates and lots of ink, and which is promising to ask for more.

E-banking and financial services refers to systems that enable banks and financial institutions' customers to access accounts and general information on bank and financial products and services through a personal computer (PC) or other intelligent device. E-banking products and services can include wholesale products for corporate customers as well as retail and financial products for consumers. Ultimately, the products and services obtained through e-banking may mirror products and services offered through other bank delivery channels. Examples of e-banking and financial services may include:

- Cash management
- Wire transfer.
- Automated clearinghouse (ACH) transactions.
- Bill presentment and payment.
- Balance inquiry.
- Funds transfer.
- Downloading transaction information.
- Bill presentment and payment.
- Loan applications.
- Investment activity.
- Other value-added services.

Banks have experimented various forms of online banking for many years. The Internet, as an enabling technology, has made banking and financial products and services available to more customers and eliminated geographic and proprietary systems barriers. With an expanded market, banks and financial institutions may also have opportunities to expand or change their product and service offerings.

Indeed, as banks and financial institutions have in their vast majority introduced new technologies for the delivery of their services, a multitude of issues have been raised, the dealing with which shall be one of the most interesting and complicated legal challenges in the coming few years.

Among these issues, concerns over security, authentication, privacy, liabilities are certainly to haunt all of providers of banking and financial services, the users thereof as well as lawmakers and practitioners.

In fact, the appropriate legal framework related to e-banking and financial services shall probably constitute one of the most critical and important elements in a country's infrastructure. Indeed, and notwithstanding the fact that most of the banks and financial institutions are already providing a considerable amount of their services through the use of new technologies, the amount of users of e-banking or financial services shall largely depend on existing domestic and international legal support provided by the laws and regulations.

Such users shall only feel comfortable in using new electronic services if they are aware of a defined legal framework that would allow them to identify their rights and obligations with the least possible uncertainties.

The same shall extend to banks and financial institutions who are today using such new technologies probably having in mind the commercial aspects of introducing new services to their clients but with serious concerns over the existence of a properly defined legal framework which by the end of the day and in the absence thereof, shall refrain them from extending the scope of their services and may also lead to disregard such use, a matter that would adversely affect their business and the quality of services provided to clients.

For these reasons, the necessity of an updating and modernization of domestic and international legal structures has been recognized as being of utmost importance in the growth of e-banking activities and transactions which would constitute one of the main components for a healthy development of these sectors.

In today's presentation, I shall attempt to bring to your attention the nature and scope of legal issues confronting e-banking and financial services development while focusing on the legal strategies that are adopted by selected Arab countries. However, and because of the lack of complete legal perspectives in most Arab countries in this concern, special emphasis shall be put on both the Lebanese and Tunisian experiences, which can be considered as leading in this respect.

II. General Overview Of Internet Banking Activities

1. Motivation for the introduction of technology

The growth of the Internet banking is due to numerous factors, including competitive cost, customer service, and demographic considerations, all of which are motivating banks to evaluate their technology and assess their electronic commerce and e-banking strategies.

Some of the market factors that may drive a bank's strategy include the following:

Competition — Studies show that competitive pressure is the primary driving force behind increasing use of e-banking technology, ranking ahead of cost reduction and revenue enhancement, in second and third place respectively. Banks see Internet banking as a way to keep existing customers and attract new ones to the bank.

Cost Efficiencies — Banks can deliver services on the Internet at transaction costs far lower than traditional brick-and-mortar branches. The actual costs to execute a transaction will vary depending on the delivery channel used. For example, according to Booz, Allen & Hamilton, as of mid-1999, the cost to deliver manual transactions at a branch was typically more than a dollar, ATM and call center transactions cost about 25 cents, and Internet transactions cost about a penny. These costs are expected to continue to decline.

Geographical Reach — E-banking services allow expanded customer contact through increased geographical reach and lower cost delivery channels. In fact some banks are doing business exclusively via the Internet — they do not have traditional banking offices and only reach their customers online. Other financial institutions are using the Internet as an alternative delivery channel to reach existing customers and attract new customers.

Branding — Relationship building is a strategic priority for many banks and financial institutions. Internet banking products can provide a means for banks to develop and maintain an ongoing relationship with their customers by offering easy access to a broad array of products and services.

2. Types of Internet banking

Understanding the various types of Internet banking products will help to assess the risks involved in such activities. Currently, the following three basic kinds of Internet banking are being employed in the marketplace:

- **Informational** — This is the basic level of e-banking services. Typically, the bank has marketing information about their products and services on a stand-alone server. The risk is relatively low, as informational systems typically have no path between the server and the bank internal network.
- **Communicative** — This type of e-banking/financial services system allows some interaction between the bank/financial institution's systems and the customer.

The interaction may be limited to electronic mail, account inquiry, loan applications, or static file updates (name and address changes). Because these servers may have a path to the bank's internal networks, the risk is higher with this configuration than with informational systems.

- Transactional — This level of e-banking services allows customers to execute transactions. Since a path typically exists between the server and the bank or outsourcer's internal network, this is the highest risk architecture and must have the strongest controls. Customer transactions can include accessing accounts, paying bills, transferring funds, etc.

III. Issues in Internet Banking and Suggested Legal Framework

Many in the banking industry expect significant growth in the use of the Internet for the purchase of goods and services and electronic data interchange. The banking industry also recognizes that the Internet must be secure to achieve a high level of confidence with both consumers and businesses.

A good management of banking products and services, especially those provided over the Internet, is fundamental to maintaining a high level of public confidence not only in the individual bank and its brand name but also in the banking system as a whole. Key components that will help maintain a high level of public confidence in an open network environment include:

- Security
- Authentication and Nonrepudiation
- Trust
- Privacy

Security is a main issue in Internet banking systems. Banks are expected to provide a level of logical and physical security adequate with the sensitivity of the information and the individual bank's risk tolerance. Some banks allow for direct dial-in access to their systems over a private network while others provide network access through the Internet.

Although the publicly accessible Internet generally may be less secure, both types of connections are vulnerable to interception and alteration. For example, hardware or software

“sniffers” can obtain passwords, account numbers, credit card numbers, etc. without regard to the means of access. Banks therefore must have a sound system of internal controls to protect against security breaches for all forms of electronic access. A sound system of preventive, detective, and corrective controls will help assure the integrity of the network and the information it handles.

Authentication and Nonrepudiation is another issue in an Internet banking system. Transactions on the Internet or any other telecommunication network must be secure to achieve a high level of public confidence. In cyberspace, as in the physical world, customers, banks, and merchants need assurances that they will receive the service as ordered or the merchandise as requested, and that they know the identity of the person they are dealing with.

Banks typically use symmetric (private key) encryption technology to secure messages and asymmetric (public/private key) cryptography to authenticate parties. Asymmetric cryptography employs two keys — a public key and a private key. These two keys are mathematically tied but one key cannot be deduced from the other. For example, to authenticate that a message came from the sender, the sender encrypts the message using their private key. Only the sender knows the private key. But, once sent, the message can be read only using the sender’s public key. Since the message can only be read using the sender’s public key, the receiver knows the message came from the expected sender.

Internet banking systems should employ a level of encryption that is appropriate to the level or risk present in the systems. In this respect, electronic signature may be one of the most reliable solutions.

Nonrepudiation is the undeniable proof of participation by both the sender and receiver in a transaction. It is the reason public key encryption was developed, i.e., to authenticate electronic messages and prevent denial or repudiation by the sender or receiver. This shall be done through the use, again, of digital signatures.

Trust is another issue in Internet banking systems. As previously noted above, public and private key cryptographic systems can be used to secure information and authenticate parties in transactions in cyberspace. A trusted third party is a necessary part of the process: the certification authority.

A certification authority is a trusted third party that verifies identities in cyberspace, functioning as an online notary. The basic concept is that a bank, or other third party, uses its good name to validate parties in transactions.

Banks also may need a way to validate themselves in cyberspace, as theft of identity has taken place. The world has witnessed cases where perpetrators have copied legitimate brokerage-firm Web sites, altered addresses for customers to contact (and send checks), then put the fraudulent Web site back on the Internet. Except for the post office box and possibly the URL, everything on the Web site could appear legitimate. Banks will have to guard against a variety of frauds as banking on the Internet becomes more prominent. A proper mix of preventive, detective, and corrective controls can help protect national banks from these pitfalls. Digital certificates may play an important role in authenticating parties and thus establishing trust in Internet banking systems.

Privacy is a consumer issue of increasing importance. Public concerns over the proper versus improper accumulation and use of personal information are likely to increase with the continued growth of electronic commerce and the Internet. The role of adequate and comprehensive Data privacy laws are becoming thus of high importance.

Accordingly, legal strategies are mainly revolving around the setting, enactment and enforcement of a set of laws comprising:

- Law on Electronic and Digital Signature
- Law or Regulation on third-party Certification Authorities
- Laws or Regulations on e-Banking per se
- Law on Data Privacy

IV. Regulatory Developments In Lebanon

In a successful attempt to reemerge to the world as an updated, technological and competitive market place, Lebanon has taken serious steps towards the modernization of its legal system.

The Lebanese government is seriously working on a legal strategy in order to modernize its laws and regulations concerning many subjects directly related to e-commerce, i.e. electronic signature, cryptography, authentication, data privacy, consumer protection, taxation, domain names, e-banking and e-financing services, e-crimes, e-government, etc.

In particular, while a number of the above mentioned topics are being subject of discussions between the government and local and international experts, many of such subjects have taken a further step and there are today draft of laws and regulations for an almost immediate application.

In this respect, Lebanon's most recent steps towards the up hauling of its legal system to accommodate new technologies and in particular in the banking and financial sectors were (i) the government approval of a draft law recognizing and legalizing electronic signatures and electronic documents, (ii) the Lebanese Central Bank Circular which regulates electronic banking and financial transactions along with its draft update, and (iii) the formation of a Committee among members of the central Bank and legal consultants for the drafting of laws and regulations which shall complete and amplify the legal framework for electronic banking and financial transactions, the "Committee on Modern Banking & Financial Techniques and Information Technology" (COBTI).

1. The Electronic Signature Law

Under a Civil Law system, and therefore having a prescriptive approach to methods of proof and authentication, Lebanon's Codes were not ready to accommodate electronic signatures.

The Lebanese proposed legislation, which is expected to be passed by the Parliament during its next session, is based essentially on the French experience and introduces various modifications to the provisions of Article 142 of the Code of Civil Procedures, inserting new articles to authentication and proof.

Under the proposed law, electronic and paper written documents shall have the same legal validity, as a way of proof.

According to Amendment (1) of Article 142, the written proof shall constitute any series of letters, forms, codes or symbols forming a readable meaning irrespectively of the medium or devices used for its formation or for its transmission.

The Lebanese legislative initiative treated the electronic signature subject with technological neutrality, meaning that it did not specify any specific authentication method in order to recognize a document or a signature.

Amendment (2) of the above mentioned Article is intended to insure that local laws do not discriminate against, or otherwise discourage the use of electronic documents, and states that an electronic document shall have the same legal presumption of a paper written document, provided that the electronic document is “capable of identifying the originator of the document and that such document was generated, stored and transmitted according to terms able to secure the validity and safety of its content”.

While the text of law does not specify any electronic authentication technique, it requires certain “security” properties of the electronic document, in order to meet the same legal presumption of a paper written document.

In the same line of non-discrimination against electronic documents, Amendment (3) determined that “in the absence of any specific rules or procedures for proof or in the absence of any adequate agreement for proving the obligations and rights of the parties, the court may settle any disputes with the respect to the written proof by defining the most credible document irrespectively of its support through any available means.”

Amendment (4) concentrated on determining the function of a signature and did not stipulate any specific form in order to validate it. It states that the function of a signature, which is associated to any kind of writing, is to identify the signer and to express his approval of the obligations resulting from such writing, regardless of its form.

Moreover, Amendment (5) states that the electronic signature is valid “when the used means and procedures are trustworthy and capable of identifying the signer and confirming the connection between the signature and the associated document”.

Once more, we notice that the legislator did not require the usage of any specific technology in order to consider valid electronic documents and signatures, establishing technological neutrality in respect to authentication mechanisms.

If reliable methods are employed, which are capable to secure the identification of the signer and at the same time is capable to confirm the connection between the signature and the associated document, such document shall be entitled to the same legal presumption attributed to hand written documents, regardless the mean or mechanism used for its creation.

The Lebanese proposed Bill on electronic signature is flexible and allows an easy adaptation of the law to all kind of existing technologies and for new technologies to be created.

The Council of Ministers, pursuant to the proposal of the Minister of Economy and Trade, shall issue decrees to set forth the rules and procedures for proving the validity of documents generated, stored and transmitted through electronic means including the rules and procedures for rejecting the electronic signature or claiming its forgery.

2. Central Bank's Circulars 1809 and 1810

The Lebanese Central Bank, on 30 March 2000, in a first attempt to modernize, regulate and organize the Lebanese electronic banking sector, issued two Circulars (Circular No. 1809 to all banks operating in Lebanon and Circular No. 1810 to banks, financial institutions and institutions dealing with electronic banking and financial transactions).

It is important to note that the Lebanese Central Bank is dully authorized to issue regulations in respect to banking and financial issues through Circulars and Decisions, which have force of law.

According to Circular No. 1809, all branch of banks operating in Lebanon shall have their network connected to the bank headquarters' network in order for all operations carried out by such a branch to be registered under the main office of such bank.

As per Circular No. 1810, all operations and activities that are concluded, carried out, or promoted through electronic or photo-electric means (telephone, computer, Internet, ATM, etc.) by banks, financial institutions, financial intermediaries, mutual funds, or any other institution or entity shall be considered "electronic financial and banking transactions".

This definition shall also apply to operations undertaken by issuers or promoters of payment and credit cards and by institutions involved in electronic transfers. It also applies to institutions involved in offering, purchasing and sale operations, and in the provision of other electronic services related to financial instruments, as well as to their settlement and compensation centers.

Among other provisions, the Circular set some principles of conduct, whereby any entity that undertakes electronic financial and banking transactions shall follow: honesty, integrity and transparency, adopting adequate procedures for ensuring maximum security, and taking all necessary measures to define and restrict various responsibilities.

Digital signatures are accepted only when they meet the following conditions (there should be a clear agreement between the concerned parties): the signatory should use a personal identification code; the institution implementing the transaction should confirm it within 24 hours by electronic mail, and within one week by regular mail, unless the client requests its mail to be kept with the said institution; and the implementing institution should provide the client with a detailed monthly statement of account, to be sent to an address of the client's choice.

Violations to these and other provisions brought by the said Circular may be sanctioned by administrative penalties.

Currently, COBTI is revising Circular No. 1810 in order to amend it through the introduction of new regulations and requirements on banks willing to provide electronic services to their clients. Mainly, new amendments shall include (i) the extension of operations covered by the new regulation to cover electronic money, mobile phone banking, WAP, credit cards, electronic trading of stocks and financial instruments, etc., (ii) the requirement of a pre-notice to the central bank prior to the actual offering of e-banking services, (iii) the requirement on foreign banks to apply for a license prior to the actual offering of e-banking services; (iv) requirements related to security procedures including a handbook from the banks Supervisory Committee, (v) other specific requirements concerning the different types of e-banking services.

3. Data Privacy Law

Recently, COBTI is preparing a proposed regulation to be issued by the Central Bank concerning Data Privacy and to be applied to banks and financial institutions.

Such proposed regulation for Data Privacy is mainly based on the European Directive on Data Protection.

In general, Lebanon does not have a Law specifically dealing with privacy of Personal Data. The only existing legal text, which roughly deals with this issue, is Law dated 3 September 1956 on Bank Secrecy.

According to Article 2 of the Bank Secrecy Law, managers and employees of the banks referred to in Article 1, as well as persons who, by nature of their position or function, have access, in a way or another, to banking records, books, operations and correspondences are bound to absolute secrecy with respect to the clients of these banks. They shall not disclose to any person or authority whatsoever, whether private, public, military or judicial, the names of such clients, their assets, or any matters related to them, unless duly authorized to do so in writing by the concerned party, his heirs, legacies, or in the event of a bankruptcy declaration or in the case of an action arising from a banking operation between the banks and their clients.

Notwithstanding such legal provision, several important issues related to data privacy are not covered by such law as: the definition of Personal Data; the issue related to who owns the Personal Data; time limit to the storage of Personal Data; the purpose of collecting Personal Data by banks; how the Personal Data is collected, processed, stored, amended and deleted; security procedures of electronic Personal Data among others.

Therefore, and in order to cover all aspects related to the data privacy, while following the basis of the European Directive, the above mentioned Committee is preparing a draft regulation to be issued by the Central Bank and to be applied to all banks and financial institutions operating in Lebanon. Such regulation is also being expected to serve as foundation to a further Law on Data Privacy to be applied not only in the banking sector, but also in all sectors which gather and store personal data.

V. Regulatory Developments In Selected Arab Countries

1. Regulatory developments in UAE

In February 2000 Dubai ruler Sheikh Maktoum bin Rashid al-Maktoum issued a Decree (the E-Commerce Law) setting up a free-trade zone for electronic commerce and technology. The decree established an independent body, the Free Zone Authority (the “Authority”) headed

by Crown Prince Sheikh Mohammed bin Rashid al-Maktoum, which would operate under the Dubai government to organize the emirate's drive to become a regional center for electronic commerce, technology and information.

Article 8 of the above mentioned Decree establishes the objectives of the Authority, which, among others, is the research, preparation and advise to the government on issues related to laws appropriate to the regulation and encouragement of Technology, Electronic Commerce and Media in the Emirates, tackling subjects as data protection and control of crimes associated with Electronic Commerce.

Accordingly, the Authority is preparing a series of laws that shall address the entire range of legal issues, specially issues such as e-security, e-signature, authentication and confidentiality of information that shall apply to banks.

2. Regulatory developments in Kuwait

In Kuwait, and through the government's view of the necessity of introducing specific amendments to existing laws in order to accommodate the use of electronic services, the Kuwaiti Chamber of Commerce and Industry (KCCI) was assigned to propose a Draft Law on electronic signatures as a first step towards providing the existing legal infrastructure with the required laws and regulations.

In fact, such Draft Law has been prepared by KCCI and submitted to the government. The basis of this Draft Law has been the UNCITRAL Model Law, however taking into consideration the specificities of the Kuwaiti legal system.

In preparing the Draft Law, KCCI has also benefited from foreign projects, mainly the Singapore Electronic Transaction Act, the Irish Electronic Commerce Act 2000 and the Tunisian Law on Electronic Exchanges and Electronic Commerce.

It is expected that the Electronic Signature Law in Kuwait shall be enacted during the current year immediately after the in depth ongoing discussion is finalized.

3. Regulatory Developments in Egypt

The Government of the Arab Republic of Egypt has also recognized the high priority of improving its legal and regulatory environment for the Information and Communication Technology sector.

To achieve this result, USAID has signed a bilateral agreement with the Egyptian Government in the view of providing the necessary funds for a project that shall allow technical assistance, training, grants and commodity procurements for the Information and Communication Technology related hardware, software and services.

The implementation of an improved legal and regulatory environment for the Information and Communication Technology is among the priority areas that shall be supported by the USAID project, and shall include the draft of telecommunications, e-commerce, and other technology related laws, regulations and procedures.

The project shall also promote a strong e-commerce environment by implementing activities that encourage electronic financial and payment services, and address security concerns such as encryption and data protection.

4. Regulatory Developments in Tunisia

The government of Tunisia has taken very important steps towards preparing the country to enter the age of electronic commerce.

In this respect, Law 2000-57 of 13 June 2000 modified and supplemented certain articles of the Code of Obligations and Contracts to include digital signatures within the chapter related to Proof.

Another initiative of the Tunisian government was the enactment of a bill regulating electronic commerce (the “Electronic Exchanges and Electronic Commerce Bill), which was adopted on 27 July 2000. This law regulates the use of the electronic commerce as well as electronic signature. This legislation is the result of three years of studies on electronic commerce carried out by a national Commission, which was created in 1997. This commission was responsible for studying the various aspects of electronic commerce and a final report was submitted to the government in March 1999. In May 1999, a ministerial consultation discussed the Commission Report and took significant measures to prepare the implementation of electronic commerce in Tunisia.

The Electronic Exchanges and Electronic Commerce Bill, while tackling electronic signatures and electronic commerce also provides for the regulation of direct related subjects such as:

- Certification Authorities;
- Electronic Contracts
- Protection of Private Data; and
- Crimes related thereto

Such legal initiatives, although not specific for banks and financial institutions, have shown that the Tunisian government is seriously engaged to the regulation of the modern forms of provision of electronic services and other financial transactions.