TECHNICAL PROTECTION FOR ELECTRONIC BANKING OPERATIONS IN JORDAN

Mohammad AL AN'IMAT[*]

ABSTRACT *:The Internet has played a major role in our daily financial business; in fact, a secure end-to-end transaction requires a secure protocol as these software-based solutions include the use of encryption algorithms, private and public keys, and digital signatures used by MasterCard and Pretty Good Privacy.*

What are the characteristics or qualities of technical protection that achieve cyber security and leadership in regulating electronic banking operations in terms of legal legislation?

This article aims to draw the attention of lawmakers to develop legal legislation on an ongoing basis to ensure the safety and stability of the accelerated electronic financial system. On the other hand, any tightening in the regulation of electronic banking services may be counterproductive because such solutions will quickly become obsolete due to the rapid pace of technological change.

The legal system of electronic banks in Jordan is based on the Electronic Transactions Law, where the Central Bank of Jordan issues legal instructions regulating electronic business and instructions for cyber adaptation in electronic payment companies.

This law includes the conditions for the Central Bank's approval of granting licenses to these companies, monitoring their compliance with them, and technical protection for customers.

KEYWORDS: *Electronic banking operations; Protections; Exchanging; License; Fraud.*
JEL Code: *K22, K34.*

1. INTRODUCTION

The importance of digital financial services and e-commerce has increased in 2020, as millions around the world are spending more time at home due to covid-19. Experts note that, in turn, has led to a sharp rise in cybercriminals' use of social engineering techniques to target users,this is why it is important for both financial institutions and customers to be aware of typical fraud tactics and schemes, and to be able to protect themselves (David Jarmon, 2002).

One of the reasons for the complexity of the work of compliance units in banks and financial institutions is the tendency to rely heavily and perhaps excessively on technology in conducting financial and banking operations, this increasing reliance on financial technology, increased association with financial technology companies, and the expansion of attributing financial operations to artificial intelligence technology, which aims to

[*] PhD- student in financial law at the Faculty of Law, University of Debrecen, HUNGARY.

reduce human intervention in banking operations with the aim of reducing cost and accelerating the completion of transactions, all of this may lead to exposure to risks beyond the cyber and information technology field.

There are two common tactics attackers use to gain access to accounts, both of which are a continuation of similar trends observed in 2019, the first scammer masquerades as a "savior" claiming to be a security expert with scenarios to save the user from imminent danger; Criminals contact bank customers pretending to be in charge of digital security, demanding fees or payments and offering them assistance.

Lifesaver may require customers to verify their identity by sending a code in a text message or app notification, to stop the transaction or transfer funds to a "secure account", They may also ask their victims to install a remote management app, pretending to need troubleshooting. Scammers often identify themselves as employees of large banks operating in the territory of their potential victims, and use a fraudulent phone identifier when calling, which indicates that the call came from a real bank number.

Online banks have to take measures to protect themselves and their customers from ever-changing fraud techniques, by limiting the number of attempts needed to make a transaction, cybercriminals may try several times before they can enter the correct login credentials, and educating customers about tricks that may be used by criminals the Internet, by regularly providing them with information on how to identify fraud and the best way to act in such situations, conducting annual security audits and penetration tests to find weaknesses in the corporate network, establishing a dedicated fraud analysis team capable of identifying and analyzing emerging methods, implementing multi-factor authentication To reduce the chance of account acquisition. measures that are used, whether in the technical or preventive fields, to preserve information, hardware and software (Al-Hamidi, 2005).

Through what is known as electronic banks, which as much as they have added facilities and speed in carrying out banking operations to obtain the service as it has become one of the most used means in various aspects of fraud, where countries and organizations have made efforts to protect the electronic banking customer are different aspects of bank fraud, especially the internal one, in which one of its employees is complicit in this crime.

2. METHODOLOGY AND DATA USED

The study relied on the descriptive analytical approach that aims to clarify the facts of things, as it was used to analyze the technical protection methods related to the subject of the research, by discussing the methods of protection currently used in electronic financial operations and forms of fraud through the Internet and recommendations using the best methods of protection and keeping pace with technological development and protection It also depends on the regulations and instructions of the Central Bank of Jordan with regard to licensing electronic banking commerce and methods of cyber adaptation and the UNCITRAL Model Law on Electronic Commerce and related laws issued by the United Nations and This study relates to the issue of electronic banks in accordance with the Jordanian Electronic Transactions Law No. 15 of 2015, and it is one of the modern topics in the field of electronic commerce and on the national scale, and against the background

of that the Electronic Transactions Law No. 15 of 2015 was approved, which constitutes an important step.

Discussing important role played by Central Bank of Jordan in protecting electronic banking operations by adapting cyber security risks and what is legislative role in issuing instructions and regulations to license and approve establishment within a series of consumer protection and electronic operations continuously in line with technological revolution facing dangers of electronic fraud and electronic attacks are increasing and Discussing Guidelines for Consumer Protection issued by United Nations in 2016.

Research objective it aims to ensure the safety and stability of the electronic financial system for electronic banks, and to follow up on the latest technical protection systems for electronic financial operations and forms of fraud through the Internet and regulatory legislation from the Central Bank of Jordan.

Research question the following problem can be posed, what are the strengths and weaknesses of the protection system in the electronic operations of electronic banks and what is the strategy by electronic banks to protect their customers?

3. THE ELECTRONIC BANKING OPERATIONS

The provision of services by banks through electronic communication networks is called electronic banking operations, and access to them is for the subscribers who are members in them according to the membership conditions determined by the banks.

It is divided into first providing information about the services provided by the bank without providing online banking services. Second: Customers obtain services such as determining their transactions and account balances, updating their data, and requesting loans.

The important thing here is when customers request the application of banking operations such as money transfer, and this requires that banks have procedures to assess, monitor and protect risks from fraud.

I.The concept of electronic banking (Ramadan, 2001):

The concept of electronic banks first includes electronic banking is conducting banking operations by electronic means, that is, using information and communication technologies and withdrawing and paying the transaction of transferring the creditor in securities, or other new business, whether it is related and in light of this type of banking services, it is not necessary to The customer has to go to the bank where he can perform some operations with the bank he deals with while he is at his home or in his office which means transcending the dimensions of time and place.

The banks that provide innovative banking services that the customer needs are called, and they are known as electronic banks via the Internet, 24/7 through the PC without any hindrance from the above, the following characteristics can be deduced; services are provided through electronic banks without time limitation The customer is from anywhere in the world via the Internet, so it is one of the aspects of international banking and the possibility of electronic delivery of some products and the high speed of performance and the Jordanian legislator has dealt with the issue of electronic banks in Articles (21 and 22) of the Jordanian Electronic Transactions Law and set conditions for licensing transfer and electronic payment companies and procedures for the work of electronic payment system.

A distinction can be made between two types of banks that practice electronic banking, which are as follows; for virtual banks or Internet banks, this type saves real estate expenses, the first Banks that do not have a fixed structure, which are electronic banks of all kinds, The second Land banks, are ordinary banks that offer electronic services in addition to their well-known traditional banking services.

II.Infrastructure of electronic banking services:

In fact, Jordan has reached an advanced infrastructure regarding digitization and its status is "excellent", and there are projects that have been implemented that do not exist in many of the surrounding countries, but this did not affect the citizen for the delay in the completion of services, and I believe that the challenge of digital transformation is procedural rather than technical.

Accomplished the Ministry of Digital Economy and Entrepreneurship in Jordan has completed 450 automated services that are widely used by citizens, pointing out that there is a tendency to cancel all information services and obtain them through the citizen's national number, whether related to social security, property, national aid, and various documents (Economy, Jordanian Ministry of Digital, 2021).

The Jordanian digital identity will be an alternative to the traditional identity in the future and will contain all information related to databases that are of interest to the citizen, which will contribute to providing services in an easy and quick way possible and at the lowest costs.

In fact, the national strategic plan for digital transformation and the executive plan until 2025, which was prepared in line with national policies and strategies and global trends in the field of digital transformation, is distributed over infrastructure and its many components, data, and the provision of legislation, especially the Personal Data Protection Law that protects people's data and prevents Any party can use it without the consent of its owner, in addition to digitizing services, and partnering with the private sector.

Establishing the rules of electronic banking and electronic commerce in general requires the creation of an infrastructure based on the technology sector. In addition to legislative and regulatory requirements that include electronic transactions with a cultural and social environment, modern information and communications are appropriate, and can be mentioned in the following (Ghannam, 2010):

III. Electronic banking basics ***:***

Existence of a wide electronic network that includes all relevant bodies then develop a phased plan to start introducing electronic banking services according to priorities and develop systems that allow linking and exchanging data between different agencies then establishment of the administrative body that coordinates between all the bodies.

IV. Types of electronic banking (Hammouri, 2010) :

There are many types of electronic banks, the most important of which are: A (Hammouri, 2010)TM service, phone bank service, call center, short message service, point of sale service, but the most famous of them are Internet banking services, which take the following forms:

Informational website: It is the basic level of electronic banks or the minimum level of electronic activity, from which the bank provides information about its services, programs and others.

The communication site: The site allows a kind of communication exchange between the bank and its customers, such as e-mail, filling out online applications or forms, or modifying the information of entries and accounts.

The exchange site: It is the level at which the bank exercises its services and activities in an electronic environment, and it allows the customer to access the management of his account by withdrawing and transferring balances, as well as controlling his financial transactions.

4. CONDITIONS FOR THE BANK TO OBTAIN A LICENSE TO PROVIDE ELECTRONIC BANKING OPERATIONS

The Jordanian legislator stipulated licensing electronic banks in accordance with "Article (31) of the Constitution and based on what was decided by the Council of Ministers on 10/18/2017, the Central Bank of Jordan issued the electronic payment and transfer system No. (111) for the year 2017 in accordance with Articles (21) and (22) From the Electronic Transactions Law No. (15) of 2015 "which deals with all issues related to licensing electronic banks in Jordan, electronic banks in Jordan are considered the same material value that is paid by traditional banks in terms of fees upon licensing, and according to the regulations issued by the Central Bank Jordanian.

For any bank to obtain a license to provide electronic banking services, it must first establish a website for itself, after obtaining a set of licenses through the following (Central Bank of Jordan , 2018):

Granting licenses is limited to banks registered with the Central Bank alone.

That the bank satisfies the regulatory controls related to the extent of its commitment to: capital adequacy, principles of loan classification, credit concentration and others.

The bank should follow the principles of risk management when providing its services through the electronic network, and the licensed bank's disclosure on its own page that it obtained a license with the number and date, in addition to linking the bank's website to the Central Bank's page.

On other hand, consumer complaints and disputes businesses should have grievance-handling mechanisms that provide consumers with a prompt, fair, transparent, inexpensive, accessible, expeditious and effective resolution of disputes without undue cost or burden, companies should consider subscribing to local and international standards relating to internal complaints handling, alternative dispute resolution services, and customer satisfaction rules (United nations Consumer Protection, 2016).

- The practical and economic importance of electronic transactions:

To name its activities and financial services via the Internet brings me the many benefits that accrue to the banks and the reductions in expenses incurred by the bank to carry out some different banking transactions without the need to move to the bank, and this leads to providing the establishment of new branches in remote areas that will not be left behind by establishing bank websites via the Internet much less From the cost of establishing a new branch for it, including buildings, trained equipment, protection and many technical sciences (Central Bank of Jordan , 2018):

entry of global banks into the Internet and perhaps enabling it to have competitive capabilities, seeds of entry are required for the rest of the banks to enter these services in order to face the new challenges arising from the offer of foreign banks the services they

are and the clients doing accordingly in comparing the services of all banks by choosing what suits them, and Enhancing intellectual capital and developing information technology.

Electronic banking aims to facilitate inter-bank dealing and make it continuous over time, shortening geographical distances and raising traditional eyebrows (Central Bank of Jordan , 2018) , and Establishing direct relationships between buyers and sellers, and Providing more job and investment opportunities, and the use of the Internet in banks is a media window to enhance transparency, by introducing these banks, promoting their services, and the media in the bank. The table is the financial indicators to put them at the disposal of researchers and scholars, and It seems that the communications and information revolution has become influential in the daily life affairs in the developed countries. It It is expected that the Internet in the coming years will be a major factor in the success and survival of the economic and banking institutions that are interested in these services, and on the contrary, they will remain far from them.

5. EXAMPLES OF ELECTRONIC BANKING FRAUD AND PROTECTION

Banking operations witnessed a remarkable development, especially after the emergence of Internet and electronic commerce networks, which enabled customers to conduct banking transactions through the websites of those banks on the Internet using special methods for traffic, which allowed fraud and its spread using the following methods (Hamad, 2017):

Credit cards that allow the withdrawal of funds, whether from their owner or through another person, or forgery, and transfer of funds, and Fraud through ATMs.

I will analyze one of the fraud cases decided by the European Court of Justice on November 11, 2020, the Court of Justice of the European Union (CJEU) held that the near-field communication (NFC) functionality of a bank card, also known as contactless payment, in itself is a "payment instrument" as defined in the EU Payment Services Directive 2015/2366 (PSD 2).

The CJEU also clarified the meaning of "anonymous use" under PSD 2 with regard to NFC functionality. The court stated that a bank may not exclude its liability for unauthorized low-value transactions in its general terms and conditions by simply claiming that blocking the NFC functionality would be technically impossible, but must prove impossibility in light of the objective state of available technical knowledge when a customer reports a lost or stolen bank card.

Furthermore, the court ruled that if the user is a consumer, general terms and conditions that provide for tacit consent to possible future amendments to such terms and conditions must comply with the standard of review set out in Directive 93/13 on consumer rights protection, not with (PSD 2) (European Union Court of Justice , 2020).

-The main types of fraud can be explained in the following (Ramadan, 2001):

Electronic phishing used by criminals to invent customers through fake websites that resemble the original websites of financial institutions and electronic banks and ask them to disclose their personal information such as account number, credit card number, password, personal identification number and other important information that customers use in electronic banks It is considered one of the most common types and is demonstrated by sending a security message asking you to confirm personal details or directing you

security questions. Then, the details that the electronic customer has confirmed are sent to the criminals who use these methods in fraud, so it is necessary to inform customers and users of electronic banking operations If such technologies are dealt with and how to deal with them so that the customer is protected and on the safe side forever, the electronic banks must provide the necessary and clear information on how to benefit and deal with the customer.

-The procedures followed by banks to protect the electronic customer are the following:

You should only access the electronic banking services of a bank you have not dealt with through the link via email, and you have to enter the electronic banking services of the bank and deal with it through the official website of the bank, and block the electronic customer from any mail or phone call he receives from any business organization or person requesting his password to be used, and use of an electronic password is unique and changes regularly. It is your duty not to disclose your electronic password to anyone, even if they are an employee of a bank.

The customer must closely monitor his transactions and review his requests and statements and check them in the credit card window on an ongoing basis, and Contact the bank when you suspect any false Egyptian communication or receipt.

Registration in electronics, such as electronic registration, to the customer's use of sites and their importance that appear to be correct, while they are fraud sites using bare servers by faring false information in them, which leads to redirecting the user to other places that will appear from your browser in the correct site, which makes electronic counterfeiting More dangerous and more difficult to detect and it targets a large group of people (Al-Najjar, 2010).

Tracking viruses and Trojan horses Viruses and programs that follow the user's computer to capture his movement on the keyboard and these systems are used by the concrete to obtain passwords or cipher keys and thus bypass other security measures and the Trojan horse is a program that appears as legitimate but performs activities Illegal when it works and can use and locate the password and make the system more vulnerable to me entering or in the future simply destroying the data on the hard disk. Electronic customers should use it. Do not use computers located in public places such as Internet cafes, airport lounges, or others. A personal firewall and anti-virus programs must be installed on an ongoing basis.

Fraud through ATMs are a simplified personal performance of cash management in allowing withdrawals and deposits outside banking working hours. However, Boxers increased the frequency of frauds through ATMs and various types of fraud such as scanning cards and recording PIN numbers.

I. Methods of protecting electronic banking operations from fraud

Hacking tools that threaten information security and require technical protection Recent years have seen the development of innovative measures to protect computer security (Rashidi, 2004) "the term software piracy has been widely used to describe the process of illegal copying of third party programs, and software francization means every unauthorized taking, appropriation, reproduction or use of an information program in the function it is intended to perform as long as the program is recognized as a valuable material. As for piracy. Informatics means copying programs illegally or obtaining stored information either directly by obtaining the password, either by trick or by conducting

experiments with the words that are used for this purpose, or indirectly by capturing the electromagnetic waves emitted from the computer and then translating them".

But many computer systems on which modern payment theory is based are still not properly secured and hackers use a variety of tools and techniques to overcome security-threatening incidents The following are the most important tools used by fraudsters across the World Wide Web that threaten the security of banking information during electronic transactions and the Internet in general (Hammad., 2007):

II. Methods of threatening information security and electronic banking operations

I would like to present the following; salami techniques, that is, the saboteur executes a set of secret codes of a computer program, causing changes so small that they are unlikely to be detected, but their cumulative effect can be significant, and backdoor or trap door. When developing a program, programmers sometimes enter code to allow them to bypass usual security measures. Once the programming is complete, the code may remain in the program either by accident or on purpose, and attackers rely on this extra code to breach security.

A masquerade and a written computer program that activates or stimulates the real program as if a program was written to activate the login screen and the connection connected to it and it actually worked the second time around, but he never knew that the first login process was a trick to get the ID, and garbage collection: The computer usually does not erase data that is no longer needed, and when the user cleans the data, the above information is not destroyed, but is available for the computer to write to later, the garbage collector steals the sensitive data, and the user says that it was deleted while it was still on the computer.

Viruses and Internet worms The word virus is used in the field of informatics to refer to all malicious programs that cause damage to automated information on processing systems (David Davies of, 1988), and viruses are characterized by rapid spread, and removing it can be costly and laborious and these programs collect the information that hackers want and then send it to them, even if there are firewalls to protect the devices from penetration.

This is due to the ability of this type to exploit weaknesses in most firewall protection programs that control the exit and imaging of information from the device or the local network by Http and Ftp, and the most famous examples of these types are Caligula, Marker, where these programs help computer hackers to Full control over any device you access. There are also programs that are able to control remotely and can harness these devices to implement the coordinated survey and disrupt the work of the famous sites (Abdel Fattah Bayoumi Hegazy, 2007).

It is usually done as a precaution against viruses using software from outside the company and virus scanners on all files that are downloaded before using them. The difference between viruses and Internet worms is that the virus needs one of the programs spread among users to embrace it. Thus, it can spread and multiply from its sides, and the most famous example of this is the "Melissa virus" and the "love virus" a computer programmer from New Jersey was arrested in April 1999. He was accused of hacking public communications and conspiring to steal computer services, the penalties for Melissa are up to 40 years in prison and a fine of about $500,000 (Al-Shammari, 2016).

As the latter needed the "Microsoft Outlook" program as an incubator for it: as for worms, they do not need any program to incubate them, and their famous "Morris worm" is their source, an example of a cyber-attack is the Morris incident, one of the first major and dangerous attacks in a network environment. In November of 1988, a 23-year-old student named Morris managed to unleash a virus known as the Morris worm over the Internet, infecting 6,000 devices to which nearly 60,000 systems were connected online. Including the organs of many institutions and government departments: losses were incurred to repair the systems and operate the damaged sites by about one hundred million dollars, in addition to sums exceeding that representing the indirect losses resulting from the failure of these systems, morris was sentenced to 3 years in prison and 10,000 fines. (Ayyad, 2006).

Trojan : "A Trojan horse is a program that vandals put hidden inside the normal programs of a facility, and the computer continues to work normally at the time" in which the cached program collects data, makes secret modifications in programs and files, recycles data, or even causes a complete cover (Hammad., 2007).

Trojans can be programmed to destroy all traces of their existence after execution. To achieve the theory of penetration through Trojan horse files, a spyware that is sent and supported by the perpetrator must be available in the victim's machine. Known as the sticky coil, and sometimes the (silent) seek, it is a patch file whose primary task is to hide the victim's (the offender) device, which is the link between it and the thief the victim (Abdel Fattah Bayoumi Hegazy, 2007).

By deleting the file immediately after discovering that it does not work, but it is too late because the patch file of this type works immediately after opening it, and if it was deleted at the end, it should be noted the need to protect any database, programs or information systems from the danger of hacker attacks, especially if related to electronic payment or electronic commerce in general.

There are other ways to plant Trojans via e-mail, such as transmission through chat, as well as by downloading some programs from an untrusted site. In addition, the Trojan can be reconfigured through macros in word processor programs. Directly to the system registry file because it performs three main things every time the device is turned on, which is to open a portal or rescuer through which to communicate, update itself and collect the updated information on the victim's device in preparation for sending it to the hacker later and update the hacker's data on the other end and The main task of the patch file, immediately upon its implantation, is to open a communication port inside the infected device that enables the beneficiary's programs (intrusion programs) to penetrate: it also performs the espionage process by recording everything that happens on the victim's device.

The following is a presentation of the most important technical protection mechanisms prepared for this;

III. Technical Protection Mechanisms for Electronic Operations the protection of electronic information related to the electronic and online banking system is of great importance because of its effects on the financial disclosure of bank customers and the reputation of the latter, and the material losses that may result from that. As a result, of the damage to the bank, it should be noted that tampering with electronic information is one of the risks resulting from the use of the Internet in the banking field. There are other risks, including what takes the form of impersonating a bank client by stealing his

passwords, or recording and re-sending some messages, in addition to the possibility of hacking the site, tampering with its contents, unauthorized use and many other risks. We will discuss the following, the most important technical mechanisms recently used:

Existing models aimed at enhancing the security of electronic banking transactions rely on different types of authentication methods, several works have been proposed to adopt OTP technology.

An OTP-based authentication model updated at each login, to access account information and suggest the use of third-level authentication for sensitive actions.

In (Hamidi, 2013), authentication can be confirmed via SMS or email also according to client needs.

And for, the authors prefer to take advantage of a combination of the advantages of the two methods, Graphic password and one time password (Alsaiari, et al., 2014).

IV. The objectives of the information security strategy objectives of the security strategy are translating and explaining security as defined in the rules, principles and higher objectives of the organization and Informing users of their responsibilities and duties towards the security of information systems, which includes individuals, devices, software, information etc... A statement of the procedures that must be followed to avoid risks and threats, and to deal with them if they occur. Determining the mechanisms through which the responsibilities and duties of each user are implemented and fulfilled.

V. Characteristics and Features of an Information Security Strategy among the characteristics of an information security strategy are the following: It must be economically appropriate (economically feasible); It must be understandable to users; It must be realistic and appropriate to the organization's positions; It must be consistent with the organization's objectives; Must be resilient and addressable Must provide reasonable protection stated management objectives Must be independent (not dependent on specific hardware or software).

Characteristics of a Good Security Policy the characteristics of a good security policy are it must be applicable, through administrative procedures and directives, and Responsibilities must be defined at all levels of the organizational structure. It must be distributed to all units of the organization, and it must be documented, and It must be flexible and efficient for as long as possible (Central Bank of Jordan , 2018).

The third requirement: the premises of the information security strategy researching policies, providing technical means and necessary measures to protect information, necessitates asking questions that would allow identifying the premises of a well-defined plan that must be prepared and adopted to ensure information security. Among the most important of these questions (David Jarmon, 2002):

Does all information require the same amount of protection? Moreover, what do we want to protect? In addition, what are the risks that could threaten the information that requires protection? What are the means of this protection? How do we act in the event of a danger occurring despite the availability of this? Does all information require the same amount of protection? And what do we want to protect?

Classification of information: person bases it on the degree of risk of information penetration:

Requires maximum protection; it is the information that results in great corruption in the event of illegal access she has and requires moderate protection; is information whose illegal access contributes to reversible corruption in some proportion, and it requires little

protection: here the losses that result from data loss are considered bad and can be processed.

6. THE LEGAL FRAMEWORK AND THE ROLE OF THE CENTRAL BANK IN THE OPERATIONS OF ELECTRONIC BANKS

The legal system of electronic banks in the Hashemite Kingdom of Jordan is based on the Electronic Transactions Law No. 15 of 2015, which is one of the modern topics in the field of electronic commerce, the Central Bank of Jordan issues regulations and instructions regulating electronic business and instructions for cyber adaptation (Central Bank of Jordan , 2018) , in electronic banks, electronic payment companies, and electronic financial banks. This law, including the fees charged by this entity for this electronic services, the procedures related to the issuance of authentication certificates, the competent authority, and the amounts that are taken for this purpose (Jordanian Electronic Transactions Law , 2015).

The most important basic procedures to complete the legal regulation of electronic banks:

Must Some basic things must be available to evaluate performance and the standard of development and protection in completing the framework of electronic banks in order to chart the methods of success and effective continuity.

Network coordination: there must be factors at the same time to achieve network coordination; Including the search for sources of electrical energy for the speed and accuracy of transferring electronic transactions.

Electronic plan management: The state has an important role in supporting the national digital entrepreneurial economy (Economy, Jordanian Ministry of Digital, 2021) ,in managing the electronic plan and protecting electronic financial security, and the state must build strong bridges between the public sector and the private sector and consumer protection, and build a relationship of mutual trust and continuous cooperation Among all the institutions of society, the Jordanian government has taken many steps to accelerate the wheel of electronic progress and mutual coordination through the so-called e-government (e-banking, Gov.Jo., 2019) .

It is necessary to advance between the government and the concerned official authorities, such as the Central Bank, which plays a major role in leading the electronic work process in order to regulate electronic work in general in Jordan.

Data protection: It is necessary to provide for all protection measures and prevent hacking and electronic piracy in light of the increase in negative electronic intelligence, and it is necessary to ensure the safety of networks from viruses and illegal intrusions.

Financial management and the human element: the qualification is necessary to provide sufficient capital in order to carry out the banking work and banking operations to the fullest, and do not forget the technical cadres who are constantly developing electronic work. On qualified technical cadres armed with advanced science (Hegazy, 2003).

Evidence: In order for proof to be achieved, legislation must work to ensure electronic proof in a form that addresses all the problems of electronic transactions (Central Bank of Jordan , 2018) . Data (13) and its amendments and the Electronic Transactions Law No. (15) of 2015, especially with regard to the electronic record and signature.

Reducing the financial cost of communications: using the lowest costs, increasing advertisements, and promoting the issue of electronic banking due to its lower financial cost.

Recently, many thefts of information and electronic data used in electronic banking transactions, and electronic payment methods in general, which prompted electronic banks and central banks to increase cyber security measures and information security strategies, which is considered economic and national security for countries and citizens, which in turn formed my motivation to write on this subject (Mahmoud Muhammad Abu Farwa, 2014).

Electronic banks or electronic payment companies, and money transfers, must work to provide a secure information environment and have all the elements of cyber security and advanced protection that renew from piracy and intrusion, and they must show these systems upon licensing, and with the request submitted to the Central Bank of Jordan, In order to grant approval of the license.

Articles (22-23) of the system issued by the Central Bank of Jordan stipulate instructions for adapting to cyber risks, which are concerned with electronic financial transactions as follows (Central Bank of Jordan , 2018)**;**

("The company shall provide the following protection controls for critical systems, and sensitive data in the company for authentication/verification of the identity of the user of those systems"):

A. Using strong and effective access controls through two or more categories of authentication (Multi-Factor Authentication) and according to the level of risk, while ensuring that they are appropriately separated in a way that reduces the possibility of others knowing one of its categories through the other, and using the necessary means and techniques to ensure Accountability and non-denial.

B. In case of the urgent need for remote access; it should be used strictly, with the need to provide access controls through means of multiple authentication / verification and the use of highly reliable cryptographic techniques, and other controls to reduce the risk of unauthorized penetration.

C. Apply security standards and global best practices when selecting password specifications.

As well as the reference to "Article No. (22) of the same system and instructions issued by the Central Bank of Jordan as follows: (The company must provide the following protection controls for information related to its business"):

A. Get rid of any sensitive information that is no longer necessary for the operation of critical operations in the company and in accordance with the laws, regulations and instructions issued in this regard.

B. Ensuring the availability of information related to the company's work, by taking backup copies of it, periodically, and in safe locations inside and outside the company's workplaces.

C. Adhering to a policy that adds data when sending messages with confidential content and encrypting those messages according to their sensitivity.

D. Activate the necessary controls to protect the confidentiality of sensitive information that is kept or transmitted through external networks, including the encryption of that information.

E. In the event that the company is unable to encrypt the sensitive information stored and used in messaging, the company must find the sensitive information in an alternative and effective way, provided that it is reviewed and approved by the Information Security Manager."

Finally, we can say that the Central Bank of Jordan has worked to provide a large number of controls and foundations that are binding on banks when submitting an application for a license. The license request, and the Central Bank of Jordan is working to develop these controls, according to the development of the wheel of technical progress and the pioneering digital economy, so that it keeps pace with scientific and technological development. The legislation issued by the Central Bank was based on Article No. (21-22) of the Electronic Transactions Law No. (15) for the year 2015. The Central Bank is keen to set controls and legislation governing electronic financial work in Jordan, and has provided all controls that work on the safety, protection and confidentiality of information and accounts for customers, so as to prevent penetration, piracy and electronic threats that may affect the pioneering digital economy in Jordan.

In fact, we need an in-depth study, taking into account the Jordanian Transactions Law of 2015and UNCITRAL International Trade Law and the United Nations Guidelines for Consumer Protection which are international comparative law, and I will mention some of them here (United nations Consumer Protection, 2016):

7. CONCLUSION

The availability of a high degree of confidence among consumers in the electronic banking market, which is characterized by good performance and transparency in the provision of financial and banking services, enhances the chances of maintaining financial stability and achieving economic growth on the other hand, and works on innovation and development in financial services and products. It works to enhance trust between electronic banks and the consumer. So that there is an effective economic environment, legislation and regulatory bodies concerned with consumer protection, and the importance of this increases in light of the rapid development in the world of electronic commerce and financial banking services, which may expose the customer to the dangers of financial fraud and looting and robbery on websites as a result of the lack of sufficient control over service providers or electronic banking operations. It is a duty to emphasize business and professional ethics for everyone who works in it under the umbrella of electronic financial operations. I have come up with some recommendations that may be useful in developing the protection system in electronic operations and banking services and maintaining confidentiality as follows.

Electronic banks in particular and network merchants in general must observe accuracy and security to ensure proper use of the network to complete electronic banking operations without allowing hackers to enter the electronic banking operations being conducted or tampering with accounts and balances. In banks, which requires updating information systems to keep pace with all technical developments and continuously absorb them and keep pace with the technological development to combat hackers in addition to combating computer viruses, which is one of the most threats facing electronic dealing. Perhaps the most important security tools in use today are firewalls and encryption.

Electronic banks must follow advanced and continuous methods of technological prevention and protection to face expected natural disasters such as humidity, heat, unexpected fires, floods, fluctuations and power outages, wars, earthquakes, etc., in order to prevent computers from being exposed to them. Damage and damage and to prevent the immediate impact of electronic banking operations.

Developing its technological infrastructure, and constantly and permanently qualifying its users, to keep pace with the continuous development in the electronic field, to be able to provide electronic banking services events to its customers. That development does not exceed it.

We advise banks to state in the contracts they conclude with customers over the network that the geographical scope is specified within the countries that are signatories to international electronic trade agreements, in order to avoid conflict with countries that do not recognize these agreements (countries are closed), since the extent of the service included in the network is the world As a whole, banks should use highly qualified individuals in the field of information technology. And scrutiny when selecting a technical supplier, to be with technical expertise, and an honorable job history, in order to reduce technical gaps that may threaten the performance of electronic banking transactions quickly and in the best possible security atmosphere.

And the legislator must realize the nature and requirements of the information age, and that there is an urgent need for an integrated set of laws that must be enacted to address all the effects of the difference in the electronic environment in. In which electronic banks operate from their traditional environment, as many existing laws appear to be invalid. Facing the various and growing problems related to the use of computers in the banking field, through the formation of a legal committee under the supervision of the Central Bank and members of banks who provide electronic service in order to disclose their need for some important matters. The legal foundations that serve the banking financial work and work on its development in order to make amendments to the electronic financial legislation that has become obsolete in proportion to the need of the present time.

And electronic banks should play a role in preparing these laws to reach sound legal results, due to their important practical experience in this regard. When building a security strategy, the answer to the three main questions must be determined: What do I want to protect? From what do I protect the information? How do I protect information?

As for the legislature, the legislator must realize the nature and requirements of the information age, and that there is an urgent need for an integrated set of laws that must be enacted to address all the effects of the difference in the electronic environment in. In which electronic banks operate from their traditional environment, as many existing laws appear to be invalid. Facing the various and growing problems related to the use of computers in the banking field, through the formation of a legal committee under the supervision of the Central Bank and members of banks who provide electronic service in order to disclose their need for some important matters. The legal foundations that serve the banking financial work and work on its development in order to make amendments to the electronic financial legislation that has become obsolete in proportion to the need of the present time.

My advice banks to state in the contracts they conclude with customers over the network that the geographical scope is specified within the countries that are signatories to international electronic trade agreements, in order to avoid conflict with countries that

do not recognize these agreements (countries are closed), since the extent of the service included in the network is the world As a whole, banks should use highly qualified individuals in the field of information technology. And scrutiny when selecting a technical supplier, to be with technical expertise, and an honorable job history, in order to reduce technical gaps that may threaten the performance of electronic banking transactions quickly and in the best possible security atmosphere.

The legislator must realize the nature and requirements of the information age, and that there is an urgent need for an integrated set of laws that must be enacted to address all the effects of the difference in the electronic environment in. In which electronic banks operate from their traditional environment, as many existing laws appear to be invalid. Facing the various and growing problems related to the use of computers in the banking field, through the formation of a legal committee under the supervision of the Central Bank and members of banks who provide electronic service in order to disclose their need for some important matters. The legal foundations that serve the banking financial work and work on its development in order to make amendments to the electronic financial legislation that has become obsolete in proportion to the need of the present time.

Finally, I hope that I have provided even a small part through this painful article in the field of electronic banking operations, to the benefit of researchers and specialists in the field of electronic banking.

REFERENCES

According to the instructions for adapting to cyber risks issued by the Central Bank of Jordan on 6/2/2018.

Al-Janabihi, Munir and Mamdouh Al-Janabihi (2005), Electronic Banks, first edition, Dar Al-Fikr Al-Jamiah, Alexandria.

Al-Najjar, Abdel Hadi (2010), Credit Cards and Electronic Banking Operations, What's New in Banking Business from the Economic and Business Perspectives, Proceedings of the Annual Scientific Conference of the Faculty of Law at Beirut Arab University, Al-Halabi Publications.

Alsaiari, H., Papadaki, M., Dowland, P. S., & Furnell, S. M. (2014). Alternative graphical authentication for online banking environments.

Application form for a license for payment and electronic money transfer companies in the Hashemite Kingdom of Jordan, issued by the Central Bank of Jordan.

B. Chaimaa & E. Najib & H. Rachid, E-banking Overview: Concepts, Challenges and Solutions, Springer science Business Media, 2020.

David Davies, Computer Virus-the major computer abuse treat of 1988.

David Jarmon , "A Preparation Guide to Information Security Policies" ,ANS Security Essentials GSEC Practical Assignment , Version 1.3, SANS Institute 2002.

David Jarmon , "A Preparation Guide to Information Security Policies" , SANS Security Essentials GSEC Practical Assignment , Version 1.3, SANS Institute 2002.

Electronic Payment System No. (111) of 2017, issued by the Central Bank of Jordan.

Ghannam, Sherif Mohamed (2010), The Bank's Responsibility for the Computer's Errors in the Electronic Transfer of Money, Dar El-Gamaa for Printing, Publishing and Distribution, Cairo.

Hamidi, N. A., Mahdi Rahimi, G. K., Nafarieh, A., Hamidi, A., & Robertson, B. (2013),Personalized Security Approaches in E-banking Employing Flask Architecture over Cloud Environment, https://www.researchgate.net/publication/275068123 _banking_Employing_Flask_Architecture_over_Cloud_Environment,[Online] Available from (Accessed 22 June 2022).

Hammouri, Nahid (2010), Electronic Business Papers, House of Culture, Amman.

Hassan Taher Daoud,(2004) Information Network Security, Institute of Public Administration, Saudi Arabia.

Khalaf Muhammad Hamad (2017), a study on liquidity risk and its impact on the profitability of commercial banks, Tikrit University, College of Administration and Economics, published, by the Journal of Baghdad College of Economic Sciences, Issue 52.

Mahmoud Muhammad Abu Farwa,, Electronic banking services via the Internet, House of Culture, Amman, Jordan, 2009.

Najm Abdullah Al-Hamidi, Management Information Systems (Contemporary Introduction), first edition, Dar Wael Publishing, Amman, Jordan 2005.

Ramadan, Medhat Abdel Halim (2001), Criminal Protection for Electronic Commerce, Dar Al-Nahda Al-Arabiya, Cairo.

Tariq Abdel-Al Hammad. E-Commerce: The Technological, Financial, Marketing and Legal Dimensions, University House, 2nd Edition, Alexandria, 2007.

The Banking Law was issued in the official newspapers issue No. (4448), dated 1/8/2000.

The electronic payment system for electronic payment and money transfer companies in the Hashemite Kingdom of Jordan, issued by the Central Bank of Jordan.

United nations Consumer Protection Guidelines United Nations, New York and Geneva, 2016.

www.alsharef.com ... See the website for more details in the field of e-commerce requirements.

www.Jordan.Gov.Jo (See the e-banking website) . https://portal.jordan.gov.jo /wps/ portal/ Home, See the E-banking website,[Online] Available from (Accessed 27 June 2022).