AL ANIMAT, MOHAMMAD

The Risks Facing Electronic Banking Operations and Legal Protection in Jordan

Introduction

Electronic payment operations have become in the minds of banks until they occupy a good position in the competition among them, and despite the fact that they are surrounded by many risks, this is called the risks of electronic payment operations, and this is what will be addressed.

Electronic banking means virtual access to bank account information. One of its main problems is the huge difference between a non-digital human connection, which uses different identification mechanisms (name, password, handwritten contract, etc.), and an electronic/digital connection that uses the authentication methods mentioned in this paper.[1]

Integration of risk management processes The electronic payment aims to ensure and define an understanding of the nature of the interrelationships between the various risks in the bank, as it is not possible to evaluate the impact of certain risks in isolation from the rest of the other risks related to the bank's work, and the risk management process is comprehensive at the level of the institution as a whole, which leads to the application of Integrated risk management, in addition to the ability to understand the interrelationships between different risks. Electronic payment operations and their attendant effects in a way that negatively affects the operations of the bank. For example, in Sri Lanka, the results of the completed study revealed that financial and security risks are taken into greater consideration by e-commerce users than other risks such as perceived, operational and financial risks.[2]

---

[1] Hanaek, Petr – Malinka, Kamil – Schafer, Jiri: *E-banking security – comparative study*. In: 42nd Annual IEEE International Arnahan Conference on Security Technology, Prague, Czech Republic, 2008. 326–330.

[2] Rajaratnam, Arthika: The Factors Influencing on Internet Banking Adoption in Trincomalee District, SRI Lanka. *International Research Journal of Advanced Engineering and Science* Vol. 4 Issue 1 (2019) 160–164.

The Basel Committee on Banking Supervision indicated that banks should put in place policies and procedures that allow them to manage these risks through their assessment, monitoring and follow-up. The Basel Committee on Banking Supervision is the committee that was established and consisted of the ten industrialized countries: Canada, Britain, France, Italy, the Netherlands, Sweden, the United States of America, Switzerland, Japan, Luxembourg, at the end of 1974, under the supervision of the Bank for International Settlements in the Swiss city of Basel, and from The most important goals of the stability of the international banking system, especially after the exacerbation of the debt crisis for the poor countries of the world.

The risk assessment should be carried out by an independent body with sufficient authority and experience to assess risks, test the effectiveness of risk management activities, and make the necessary recommendations to ensure the effectiveness of the risk management framework.[3]

There must be plans reinforced with preventive measures against crises, to be approved by the concerned officials, to ensure the bank's ability to withstand any crisis or failure in the systems or communication devices, provided that these plans are subject to periodic testing.

Data and Methodology of study used

The research depends on the descriptive analytical approach to verify the most important risks facing electronic payment operations. These risks are analyzed and taken advantage of to keep pace with modern protection methods related to the topic of research, discuss the most important forms of financial fraud, and develop the best recommendations for the use of protection methods and keeping pace with high technological development.

And review the laws issued by the Central Bank of Jordan and the instructions for cyber risks according to the Central Bank of Jordan and what is related to the licensing of electronic banks and the regulations issued by The Basel Committee on Banking Supervision (BCBS) in addition to the laws issued by the United Nations[4] to protect against risks that threaten consumers in the field of cyber security and electronic commerce.

The policy of the Jordanian government measures

Remittances outside the country are considered one of the most important risks facing electronic banks, which may cause great harm to the economy inside the country. Which he enjoys, but at the same time, he may be exposed to great risks, whether at the level of maintaining that good money from the banks or the economy of countries as a whole.

Threats should not affect or limit the spread of electronic payment operations. Rather, governments and legislative councils that are concerned with protecting the interests of customers and citizens, which may be represented by the Ministry of Investment

---

[3] Instructions for adapting to cyber risks issued by the Central Bank of Jordan on 6/2/2018.

[4] UNCITRAL Model Law on Electronic Commerce New York, 1996. 11.

and the Central Bank, should take into account these risks, and develop the necessary technology to prevent their occurrence on an ongoing basis and binding on electronic financial companies, by reducing its incidence to the lowest possible degree.

Jordan's policy was to protect customers from the risks of electronic fraud through the application of general rules to protect customers and citizens through the role of the Central Bank of Jordan in regulating electronic payment methods for banks, the Jordanian government encouraged citizens to go to electronic transactions and provided them with all means of protection from electronic risks. It has worked to promote the e-government program and electronic payment through the application (e-Fawateercom).[5]

In fact, the Central Bank of Jordan has developed a legal regulation regulating the work of electronic companies, electronic banks, traditional banks, electronic payment companies, and electronic transfer companies. Electronic payment is up and running. This definition legally applies to electronic banks, because it deals with the same systems and manages them electronically, and these electronic companies are not entitled to a license except after obtaining the approval of the Central Bank and submitting an application for a license through which the Central Bank requires its supervision and follow-up on the operations of the electronic bank.[6]

The researcher believes that subjecting traditional or electronic banks to the control of the Central Bank secures the necessary protection for customers, and cultivates a kind of confidence towards modern electronic payment processes that are dealt with behind screens. The Central Bank has taken over the protection of customers by enacting instructions and regulations to compel electronic financial companies to protect customers.

The legislative framework of the Central Bank appears by issuing the appropriate regulations, instructions and circulars for the activities of payment services and electronic money transfer in Jordan, defining the terms of dealing with them, settling disputes that arise between its parties, in addition to the technical and technical procedures and requirements for electronic money. Payment tools and directing those who engage in such activities to comply with them.

Regulatory framework: The regulatory framework in the Central Bank is to supervise all electronic payment systems and monitor all activities of managers and operators of electronic payment systems, participants in them and providers of electronic payment services.

It is possible to count as an example one of the largest electronic banks in the world in terms of definition and electronic payment methods provided through it to most countries of the world and the legislative texts to protect the electronic financial system and the licenses that had to be obtained from the Central Bank of Lithuania to license a Revolut bank, s a financial technology company that provides banking services in Europe and the world.

---

[5] https://bankofjordan.com/ar/digital-banking/e-fawateercom (30.05.2022).

[6] View the application form for licensing payment companies and electronic money transfer in the Hashemite Kingdom of Jordan, issued by the Central Bank of Jordan. Ammam, 2015. 17.

License conditions for providing banking operations in digital banks

The Jordanian legislator determined the licensing of digital 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 Law No. (111) of 2017 in accordance with Articles (21) and (22) From the Electronic Transactions Law No. (15) of 2015 which deals with all matters related to licensing electronic banks in Jordan, electronic banks are considered in Jordan. The same material value that traditional banks pay in terms of fees upon licensing and in accordance with the regulations issued by the Central Bank of Jordan.[7]

In order for a bank to obtain a license to provide electronic banking services, it must first create a website for itself, after obtaining a set of licenses through the following: Granting licenses is limited to banks registered with the Central Bank alone. That the bank fulfill the regulatory controls related to the extent of its commitment to the following: capital adequacy, principles of loan classification, credit concentration and others. The bank follows the principles of risk management when providing its services via the electronic network, and the licensed bank disclosed on its own page that it obtained a license by number and date, in addition to linking the bank's website to the central bank page.

Businesses should have mechanisms in place to handle complaints that provide consumers with a prompt, fair, transparent, inexpensive, accessible, rapid and effective resolution of disputes without undue cost or burden. Companies should consider subscribing to local and international standards related to internal complaints handling, alternative dispute resolution services, customer satisfaction rules and providing all means of protection against cyber risks to these processes.[8]

The Necessity of Creating a Regulatory Legal Legislation

When we research the extent to which the legal legislation covers the issues of the risks of electronic payment methods.

In fact, in Jordan there is the Cybercrime Law of 2015 and it is the authorized legislation that addresses the risks that arise from electronic operations in general, The electronic services provided by banks are characterized by speed, flexibility and simplicity, and therefore this matter required the existence of legal legislation that protects and cultivates confidence by customers in these banks and solve any dilemma he needs, hence the need for the intervention of central banks in the countries, in order to establish a legislative legal organization that cultivates confidence in the customer and forces electronic banks to apply the legal foundations regulated by the Central Bank to protect the interests of all parties,[9] and from For that, some international

---

[7] 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 Law No. (111) of 2017.

[8] United nations Consumer Protection Guidelines United Nations. New York and Geneva, 2016. 10.

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

models of the extent of central bank control over the legal regulation of banks will be studied.

The Jordanian Electronic Transactions Law requires these companies to obtain a license From the Central Bank of Jordan, where Article (22) of it stipulates the following:[10]

a) Without prejudice to any law, every payment and electronic money transfer company must obtain License from the Central Bank of Jordan.
b) Payment and electronic funds transfer companies, in carrying out their activities, are subject to the supervision of the Central Bank, the Jordanian and his knowledge.
c) For the purposes of this article, a payment and electronic transfer of funds company means the company that practices Payment services, transfer, financial settlement, electronic clearing, or issuance of payment tools and systems and its management in accordance with the provisions of this law and the regulations and instructions issued pursuant to it or the legislation other related matters.

In fact, we need an in-depth study, taking into account the Jordanian Transactions Law of 2015 and UNCITRAL International Trade Law, and the United Nations Guidelines for Consumer Protection, which are international comparative laws.[11] Consumer privacy and data security. And the terms of the contract are clear, concise, easy to understand, and unfair. Finally, clear and timely information enables consumers to easily contact businesses.

Legal Principles

At the legislative level, the legislator must realize the nature and requirements of the information age, and that there is an urgent need for an integrated package of laws that must be enacted to address all the effects of the difference in the electronic environment in which it is located. Banks operate from their traditional environment, where 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 services 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 current time.

General legal principles must be observed in protecting customers from electronic risks. The responsibility for risks lies primarily with the board of directors of each bank, which is responsible to the shareholders about the bank's business, which requires an understanding of the risks faced by the bank and ensuring that it operates in an effective manner. Accordingly, the risk Policies are set by the bank's senior management, and the board of directors must review them. The risk management policies must include defining

---

[10] Article No. 22 of the Jordanian Electronic Transactions Law No. 15 of 2015 issued in the official newspaper.

[11] United nations Consumer Protection Guidelines United Nations. New York and Geneva, 2016. 11.

or defining risks and methods or managing and controlling the risks facing electronic payment operations because the most important characteristics that encourage the adoption of electronic banking services are convenience and ease of use[12], the general legal principles in protecting customers from electronic risks issued by the Basel Committee must take into account many tasks and duties.

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).[13]

Conclusion

Through this study, the researcher can extract and suggest a set of relevant findings and recommendations to generalize and consolidate the interest as follows:

In fact, according to my opinion, banks should prepare qualified banking human cadres to work in the face of risks that threaten electronic payment operations, taking into account accuracy and security to ensure proper use of the network to complete electronic payment operations. Or tampering with accounts and balances in banks that require 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

Its technological infrastructure is well-developed in order to be able to provide electronic banking services events to its customers.

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

---

[12] Jiaqin, Yang – Li, Cheng – Xia, Luo: A comparative study on e-banking services between China and USA. *International Journal of Electronic Finance* (3) (2009) 235–252.

[13] European Court of Justice Rules on Liability of Banks for Unauthorized Low-Value Transactions Using Contactless Payment. Library of Congress, Vienna, 2020. 11.

to international electronic trade agreements, in order to avoid conflict with countries that do not recognize these agreements since the scope of the service listed on the network is all over the world. Choosing a technical supplier, provided that he has the technical expertise and honorable career history.

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.

At the legislative level, the legislator must realize the nature and requirements of the information age, and that there is an urgent need for an integrated package of laws that must be enacted to address all the effects of the difference, as many of the current laws seem to be invalid, to face the various and growing problems related to the banking field, by forming a legal committee under the supervision of the Central Bank and members of banks who provide the electronic service to disclose their need for some 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, including It fits the needs of the time. Rather, electronic banks should play a role in preparing these laws to reach sound legal results, given their important practical experience in this regard.