DOCTORAL (PhD)
DISSERTATION

Mohammad Elayan Al Animat

DEBRECEN

2025

UNIVERSITY OF DEBRECEN

MARTON GÉZA DOCTORAL SCHOOL OF LEGAL STUDIES

CHALLENGES FACING THE LEGAL REGULATION OF ELECTRONIC BANKS, UNDER THE JORDANIAN ELECTRONIC TRANSACTIONS LAW IN LIGHT OF EU DIRECTIVE AND INTERNATIONAL LEGAL STANDARDS

Candidate:

Mohammad Elayan Al animat

Supervisor:

Dr. habil. Bordás Péter PhD

Associate Professor of Law

Doctoral Program: Changes in State and Law in Central and Eastern Europe Head of the Doctoral School: Prof. Dr. József Szabadfalvi, DSc, Professor of Law

Manuscript completed on 31 January 2025

PLAGIARISM DECLARATION

I, the undersigned Mohammad Elayan Al Animat by signing the present statement declare that the thesis, entitled *CHALLENGES FACING THE LEGAL REGULATION OF ELECTRONIC BANKS, UNDER THE JORDANIAN ELECTRONIC TRANSACTIONS LAW IN LIGHT OF EU DIRECTIVE AND INTERNATIONAL LEGAL STANDARDS* - is my independent work.

In the course of preparing the thesis, I conformed to the rules of Act No. LXXVI of 1999 on Copyright, and the regulations of the University of Debrecen regarding the principles of preparing the thesis, particularly in respect of references and citations.

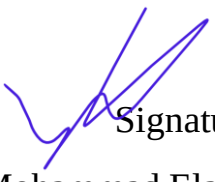
I declare moreover that in the course of preparing the thesis, in view of the condition of independent work, I did not mislead my supervisors.

I also declare that the submitted thesis in paper form and its electronic version are the same in every aspect (see Rules and Regulations, Article 24, Section 8).

By signing the present statement, I notice that the University of Debrecen has the right to deny the acceptance of the thesis and take disciplinary action against me if it is demonstrably not my intellectual creation and if any infringement of copyright falls under suspicion.

The denial of the acceptance of the thesis and the disciplinary procedure does not affect other legal consequences caused by the infringement of copyright.

Debrecen, 31 January 2025.



Signature

Mohammad Elayan Al Animat

SUPERVISOR'S RECOMMENDATION

I recommend this doctoral dissertation under the title "*Challenges Facing The Legal Regulation of Electronic Banks, Under The Jordanian Electronic Transactions Law In Light of EU Directive And International Legal Standards*" written by Mohammad Elayan Al Animat.

Digital money and e-banking have come to the fore in the 21st century, especially after the COVID-19 pandemic. However, this development also poses a number of challenges for legislators. The rules applicable to traditional banks are only partially applicable to electronic banks.

Mohammad has undertaken a thorough examination of this new area of law. The dissertation is essentially based on a comparative legal analysis, focusing on electronic banking regulation in Jordan and the EU. The research hypotheses raise a number of exciting research questions, and the research methodology is appropriate for proving the hypotheses.

In my opinion, the structure of the dissertation is appropriate and the referencing system is good. Besides the introduction and the summary, the dissertation consists of four major chapters focused on electronic banks compared to traditional banks, particularly within the context of Jordan and international practices. Chapter One introduces the differences, advantages, and disadvantages between electronic and conventional banks, highlighting their impact on customers, investors, and the national economy. Chapter Two discusses challenges in electronic banking, including security issues, legal regulations in Jordan and the EU, and the impact of international law on drafting Jordanian Transaction Law. Chapter Three explores government policies related to financial stability, monetary policies, and the influence of religious and ideological beliefs on these policies. It compares the European and American models, especially in light of the economic challenges posed by the COVID-19 pandemic. Chapter Four provides a case study on Revolut Bank, examining its financial performance, expansion, and legal challenges during the pandemic. The chapter also discusses how the bank's experience can inform the development of electronic banking in Jordan.

Mohammad's research found that Jordan's Electronic Transactions Law, particularly Law No. 15 of 2015, and the Jordanian Banking Law are not aligned with international standards, specifically the European Union's framework, in addressing the challenges of electronic banking. The laws fail to mention digital or electronic banks, focusing instead on electronic companies and services. This gap in the legal framework may lead to future legal disputes as there is no clear legislation governing electronic banks in Jordan.

Mohammad draws the following main conclusions in his thesis. The Jordanian Electronic Transactions Law - as stated by Mohammad - lacks specific provisions for electronic banks, civil liability for authentication service providers, and clear procedures for issuing electronic certificates. The EU's directive on unfair terms could be relevant for customer-supplier relationships in electronic transactions. Jordan has made progress in regulating electronic payments, but there is still a need for specific regulations for electronic banks. Electronic banks are particularly vulnerable to money laundering and cyber-attacks. Criminal protection for electronic banking in Jordan is insufficient and should be expanded to cover all electronic cards and fraud activities. Jordanian legislation lacks independent legal provisions for resolving electronic transaction disputes, unlike the more developed EU framework. These conclusions are the main findings of the research. The research emphasizes the need for Jordan to align its legislation with international standards to support the development and regulation of electronic banking.

I honestly think, that Mohammad Elayan Al Animat has worked properly on his dissertation, he showed a researcher's attitude of good niveau. The complex approach of the research theme proves the novelty of the present work. The dissertation meets all the necessary requirement, as the supervisor of the research, I support the acceptance of the dissertation for the final defense.

Debrecen, 31 January 2025.

Dr. Péter Bordás, habil., Ph.D.
Associate Professor of Law

Table of Contents

Abbreviations

AFI	Alliance For Financial Inclusion	**PCI DSS**	Payment Card Industry Data Security Standard
AI	Artificial Intelligence	**PISP**	Payment Initiation Service Providers
AISP	Account Information Service Providers	**PSD**	Payment Services Directive
AML	Anti-Money Laundering	**REG TECH**	Regulatory Technology
CDD	Customer Due Diligence	**RTS**	Regulatory Technical Standards
CFT	Combating The Financing Of Terrorism	**SCA**	Strong Customer Authentication
CFT	Combating The Financing Of Terrorism	**SEPA**	Single Payments Area
CJEU	Court Of Justice Of The European Union	**SME**	Small And Medium-Sized Enterprises
CMA	Consumer & Market Authority	**SSL**	Secure Sockets Layer
DDOS	Distributed Denial Of Service	**STR**	Suspicious Transaction Reports
EBA	European Banking Authority	**TFEU**	Treaty On The Functioning Of The European Union
ECB	European Central Bank	**TLS**	Transport Layer Security

ECN	Electronic Communications Network	**TPP**	Third-Party Payment Service Providers
ELMI	Electronic Money Institutions	**VA**	Virtual Assets
FATF	Financial Action Task Force	**VASP**	Virtual Asset Service Providers
FATF	Financial Action Task Force	**ML**	Money Laundering
FCA	Financial Supervisory Authority	**NFC**	Near Field Communication
FDIC	Federal Deposit Insurance Corporation	**ILCE**	Institute Of Economic Crime Investigation
FED	United States Central Bank	**IT**	Information Technology
FIU	Financial Intelligence Units	**ITU**	International Telecommunication Union
GDP	Gross Domestic Product	**JDM**	Judgment And Decision-Making
GDPR	General Data Protection Regulation	**JOPACC**	Jordan Payments & Clearing Company
GPFI	Global Partnership For Financial Inclusion	**KYC**	Know Your Customer
ICT	Information And Communications Technology	**MIFID**	Markets In Financial Instruments Directive
RTS	Regulatory Technical Standards	**XS2A**	Access to Account

Introduction

The competition between banks has intensified with the increasing popularity of electronic financial operations. While there are numerous risks involved, the most notable being in electronic financial transactions, electronic banking services offer convenient virtual access to bank account information. A key concern is the substantial contrast between traditional human communication, which utilizes various identification methods (such as name, password, and handwritten contracts), and electronic communication, which relies on authentication methods.[1] This research aims to explore and address these concerns.

The COVID-19 pandemic has expedited the advancement of electronic banking services, enabling customers to conveniently access financial services from any location and at any time. This has been made possible through various digital platforms, including mobile applications, websites, and electronic banking applications. As a result, there has been a rise in interest rates on savings accounts, a reduction in fees, and the introduction of competitive loan rates. E-banking plays a crucial role in promoting financial inclusion by extending services to marginalized communities and removing geographical barriers. The pandemic has sped up the implementation of electronic banking services due to social distancing measures and movement restrictions. This shift to remote services has highlighted the importance of a robust digital infrastructure. Increased concerns about virus transmission through physical contact have led to a rise in the adoption of contactless payment methods like mobile wallets and QR code payments. The expansion of e-banking has been fueled by technological advancements, changing customer preferences, and the demand for fast and easily accessible banking services.

Electronic banks play a vital role in facilitating investments and improving the movement of funds, which can have a positive impact on the country's economy and help address unemployment problems. They facilitate convenient access to financial services, thereby promoting greater participation in financial endeavors such as investment and savings. Diversifying portfolios could lead to greater returns on savings, boost economic growth, and reduce unemployment. E-banks enable the movement of capital between countries, which attracts international investment and reduces transaction-related expenses. It provides

[1] Petr H., M. Kamel, and Jiri S. "E-banking Security: A Comparative Study." In *4 2nd Annual IEEE International Conference on Security Technology*, Prague, Czech Republic, 2008. p. 326-330.

customized financing solutions for SMEs as well as startups, facilitating business creation and job generation. E-banking facilitates financial inclusion by expanding its services to marginalized people, thereby enabling them to participate more actively in economic activities. This innovation enhances efficiency in financial transactions and services, thereby increasing productivity and contributing to economic growth. Advances in fintech have the potential for new industries to emerge and employment prospects.

Since the balanced model has been considered in this research, the objectives it seeks to address multiple concerns: the protection of customer rights in electronic banks, the interests of electronic bankers and investors, and economic variables. From this perspective, my hypothesis defines the direct relationship between the challenges of e-banking and the ever-changing government policies to reconcile these conflicting parties. Therefore, I expect that the continued neglect of the emerging challenges in the financial digital environment without creating renewed legislation to keep pace with the rapid development of the financial digital transformation of electronic banks will have a negative impact on the development of this sector and its non-spread and the negative effects on society and the state, and therefore on traditional banks.

It is important to remember that international standards often remain theoretical unless their true nature is established in a practical model. Some international standards have established general principles and guidelines, focusing on security and flexibility. The integration of these aspects is deliberately left to a working model. Therefore, it is essential to refer to international standards governing the compatibility and harmonization of the Jordanian Electronic Transactions Law No. 15 of 2015 in order to develop a balanced model. This model will help the Jordanian legislator regulate a law that governs electronic banks and promotes investment in them, making electronic transactions widely available.

In addition to, the dissertation investigates the impact of EU rules on Jordanian legal frameworks, focusing on how these laws affect the formulation and implementation of the Jordanian Electronic Transactions Law. It critically assesses the viability of EU law as a comparable benchmark for Jordan, taking into account the country's non-EU status and distinct socioeconomic circumstances. Furthermore, the dissertation investigates the extent to which Jordanian regulations fit with global banking service needs, highlighting both the progress made and the problems encountered in reaching regulatory compliance with international standards.

The analysis of the impact of EU regulation on Jordanian regulation is rooted in the unique nature of this relationship and its broader implications for Jordan's regulatory framework. EU regulations often serve as a benchmark or reference point for non-EU countries, particularly in regions seeking to align with international standards such as Jordan. In fact, this analysis aims to highlight the ways in which EU regulatory frameworks influence Jordanian law, whether through direct adoption, indirect harmonization, or comparative divergence; such a focused discussion is particularly relevant given Jordan's engagement with international regulatory frameworks and its efforts to modernize its legal system in line with global standards. This analysis allows for a comprehensive exploration of these dynamics without conflating them with broader domestic regulatory developments.

The controversy surrounding the need for a complex body of legislation in line with the rapid development of the electronic banking sector is currently not limited to the mere monitoring of contractual arrangements and electronic transaction legislation; it is based on multiple arguments. At first glance, each argument can be considered counter-argument, but in the end, it can be combined with each other, serving multiple goals. While arguments for customer protection tend to enact strict rules that expand the scope of customer protection, arguments regarding the flexibility of the e-banking market tend to relax protectionist rules to stimulate the electronic transaction market. The two different arguments can be combined into a balanced model that can protect customers in their digital financial space in an active and flexible labor market. Hence, the compatibility and harmonization of Jordanian laws and the "Jordanian Electronic Transactions Law No. 15 of 2015" with the developments of the challenges and risks of the digital revolution in electronic banks and their digital applications through legislation in line with the rapid development of the electronic banking sector must be analyzed. The first is the humanitarian perspective to protect the customers associated with this electronic bank who have given it confidence and retained their balances as a vulnerable party in a contractual relationship. The second is the managerial perspective to enable investors to manage the electronic bank in a way that seeks to expand, distribute and constrain it in a way that leads to its failure. The third is the economic perspective to actively maintain the e-commerce market for sustainable development and open the spread of this sector and its positive impact on digital entrepreneurship.

1. Research Problem and Questions

It is important to consider the balanced model in electronic banking, which aims to address various concerns such as customer rights protection, the interests of e-bankers and investors, and economic variables. Regulators, particularly central banks, need to demonstrate how to level the playing field between traditional and electronic banks. This involves addressing issues such as licensing, capital requirements, competitiveness, and the benefits of transitioning from the traditional environment to digital finance. Some argue that there are numerous obstacles and increasing risks in the electronic banking industry, which have repercussions on the sector. It is essential to ensure alignment between regulations and laws governing this sector and to continuously improve to keep pace with rapid development and transformation. Neglecting the emerging challenges in the digital financial environment without introducing new legislation to keep up with the rapid development of financial digital transformation has a negative impact on the sector's development, its reach, and has adverse effects on society, the state, and traditional banks.

The purpose of this research is to highlight the challenges involved in the legal regulation of electronic banks in Jordan. It will focus on the inadequacy of the legislation that regulates these banks. In order to achieve this purpose, the research will attempt to answer the following question:

The main question: To what extent is the Jordanian Electronic Transactions Law compatible with the rapid legislative developments of this sector in light of the transformation of international standards and the European Union to address the emerging challenges of electronic banks?

The following sub-questions arise from the main question:

The first sub-question: To what extent does the Jordanian Electronic Transactions Law conform to the rapid legislative developments of electronic banks in light of international regulatory developments and the European Union?

The second sub-question: What weaknesses does the Jordanian Electronic Transactions Law include in light of the international model and directives of the European Union?

Third sub-question: What are the regulatory challenges and risks facing independent e-banks and their protection?

2. The Significance of the Research

The significance of the research stems from two aspects: theoretical importance and applied importance.

Theoretical significance

The research's significance lies in its exploration of a crucial aspect of the banking industry, which is intertwined with various regulatory, legislative, and technological variables. It also delves into the impact of these factors on performance and effectiveness in achieving goals, while identifying the role of electronic banks in the sector. The theoretical significance of the research lies in its contribution to the theoretical aspect of this field and its potential as a reference for future researchers. This topic's importance is evident in addressing the challenges faced by electronic banks, such as enhancing security, improving customer experiences, ensuring compliance with regulations, and increasing competitiveness in the electronic financial market. Additionally, it aims to explore the emerging challenges of electronic banks and assess the compatibility of the Jordanian Electronic Transactions Law with the rapid legislative developments in this sector.

Significance of the Research

The significance of the research stems from the importance of electronic banking and the role it plays in adapting the banking sector to all current developments, variables and challenges by valuing and refining the skills, knowledge and performance of its employees to achieve the conditions of administrative, legal and financial success of the e-bank experience governed by successful global experiences in all its aspects, in addition to drawing the attention of legislators to the importance of technological development in the banking sector, while emphasizing the need to adopt a serious legal system in developing and investing in them for the advantage of the dimension. legal and considering them as a tributary to the banking sector. and diversification of banking services.

3. Aim of the Research

The following points need to be considered:

- The dissertation aims to shed light and discuss the academic challenges posed by the financial technology sector to judicial authorities and legislators in general, and to discuss the legal framework for electronic banks according to the Jordanian Electronic Transactions Law and international and European Union legislation in particular, and the benefits of the transition from the traditional environment to digital finance. Regulatory authorities, especially central banks, must clarify how to achieve equal opportunities between traditional and electronic banks according to the regulations and instructions of central banks.

- Identify the extent to which Jordanian legislation is compatible with international legislation in regulating and responsibilities of the electronic signature authentication service provider, according to the Jordanian Electronic Transactions Law and international and European Union legislation, as the thesis focuses on a particularly important part of the work, which is the analysis of both civil and criminal liability of service providers and a discussion of the risks related to money laundering, which is of great importance and relevance, especially in light of the growing regulatory authorities in this field in the European Union.

- This research also aims to shed light on the challenges facing the legal regulation of electronic banks in Jordan, and will focus on the inadequacy of legislation regulating these electronic banks, and how to protect these transactions from a technical and legal standpoint.

-The dissertation will seek to conduct a detailed analysis of the EU payment system, which is considered advanced and modern, to serve as a motivating and guiding tool for the Jordanian legislator to implement appropriate systems in Jordan.

- discussing the risks related to money laundering that are growing in the electronic banking sector, which is of great importance and closely related to the difficulties in complying with many financial rules, anti-money laundering requirements and customer knowledge and the need to develop comprehensive strategies to manage their transaction scenarios, especially in light of the growth of regulatory bodies in this field in the European Union.

- Highlighting the scientific and legal addition in the field of electronic banking services, especially for lawyers, judges and employees of electronic banks. The theoretical importance of the research lies in its contribution to the theoretical aspect of this field as a reference for future researchers and the impact of the Electronic Transactions Law on electronic banking operations, with a focus on the importance of qualifying and training employees working in the electronic banking sector to keep pace with the challenges and threats facing this important sector.

- Research and discuss the legal regulations of electronic banks to address legislative restrictions and compare them with international legislation and international financial organizations in this vital sector to keep pace with the rapid development and aims to address various concerns such as protecting customer rights, the interests of electronic bankers and investors, and economic variables

4. Hypotheses of the Research

Based on the problem of the research and its questions, the following hypotheses were formulated.

Key hypothesis: Legislation has been implemented to limit identity theft and fraud in online banking. However, authorities are encountering challenges in establishing secure and authenticated digital identity procedures. New laws have been introduced to protect electronic bank customers, ensuring transparency in fees, conditions, and dispute resolution systems.

The following sub-hypotheses emerge from the main hypothesis:

First Sub-Hypothesis: There is an inverse relationship between assessing potential systemic risks associated with electronic banks and developing risk management procedures to ensure financial stability amid the growth of the cyber insurance market, and regulation to reduce risk.

Second Sub-Hypothesis: Regulators face greater difficulties in protecting the security of customer accounts and assessing the potential systemic risks associated with electronic banks, in light of the question of the responsibility of electronic banks towards customers as a powerful and dominant party.

Third Sub-Hypothesis: Additional qualification requirements are needed for employees working in electronic banks related to preventing involvement amid accelerating threats such as money laundering.

Fourth Sub-Hypothesis: Regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system.

Fifth Sub-Hypothesis: International coordination and cooperation between regulators is needed for the proper international management of electronic banks, which may lead to a combination of legislative regulations; and different jurisdictions to adapt and define appropriate jurisdiction and criteria for disputes involving e-banks.

Sixth Sub-Hypothesis: E-banks will face difficulties in complying with several financial rules, such as anti-money laundering (AML) and know-your-customer requirements, and the need to develop comprehensive strategies to manage their transaction scenarios.

Seventh Sub-Hypothesis: Is the Jordanian Electronic Transactions Law compatible with European Union and international standards.

Eighth Sub-Hypothesis: The extent to which EU regulations affect Jordanian regulatory frameworks, particularly in the context of challenges related to digital banking services, in terms of EU legislation being the most appropriate standard for Jordan, given its membership outside of the EU, and how the Jordanian banking system also meets the requirements of the global banking system.

5. Methodology of the Research

The researcher is using a comparative descriptive approach in this research due to its multidisciplinary nature. The research aims to address a problem from various angles, drawing from fields such as law and economics, in order to arrive at a scientific solution based on a sound scientific model. The research also aims to argue, similar to "*Gestel & Micklitz*," [2] that old law jurisprudence has evolved in the United States and Europe. There are ongoing debates about

[2] Rob van Gestel, Hans-W. Micklitz, and Edward L. Rubin, eds." *Rethinking Legal Scholarship: A Transatlantic Dialogue".* New York: Cambridge University Press, 2017. p.14.

replacing this type of curriculum with a multidisciplinary approach. Many academic institutions and renowned academics are now focusing on this approach. Interdisciplinary research involves examining a subject from various perspectives, allowing for the exchange of experiences across different sectors to develop appropriate solutions. This approach is crucial in the field of law due to its involvement in various aspects of life, including the political, social, economic, and institutional spheres. This strategy is crucial in the current situation because the challenges and threats caused by the digital revolution in electronic banking include not only legal principles, but also economic principles. Legal scholars tend to advocate for protecting customers from issues in e-banking, while economists argue for easing protections and reducing restrictions on the digital industry. The researcher uses the comparative approach to analyze legal documents, case studies, literature reviews, and data analysis. The research mostly involves analyzing texts and words to understand ideas, concepts, or experiences in order to prove concepts and evaluate the thesis hypotheses, The dissertation also looks into the impact of EU regulations on Jordanian legislation, specifically the Jordanian Electronic Transactions Law, assessing its suitability as a benchmark for comparison, and evaluating Jordanian legislation's integration with global banking service requirements. This strategy will continuously provide support for our research findings beyond simply clarifying applicable law. This method is famous for using basic legal principles, many types of data, and compelling arguments to influence readers toward the conclusions of the research. The descriptive method is increasingly using a multidisciplinary approach in the EU to address challenges in e-banking. This approach combines legal and economic arguments to explain issues related to common policies, which focuses on assessing the compatibility of Jordanian legislation, specifically the Jordanian Electronic Transactions Law No. 15 of 2015, with the evolving challenges and risks posed by the digital revolution in electronic banking, and the researcher's use of a comparative method by examining Jordanian and international legal sources, EU directives, and case law.

6. Research Structure

The research consists of five chapters, along with the introduction, conclusions, and recommendations; the organization of this work has been carefully planned to ensure a comprehensive examination of the topic. Specifically, the first two chapters are significantly

more comprehensive than the following chapters, a deliberate decision made to create a strong foundation and framework for the subsequent ones. The introductory chapters include essential background material, theoretical frameworks, and key concepts necessary to understand the more detailed and sophisticated subsequent analysis. By providing readers with this background knowledge in advance, they are better prepared to understand the complexities and nuances discussed in the subsequent chapters. This structure not only improves the logical flow and clarity of the text, but also facilitates the gradual exploration of the issue. The introductory chapters provide a comprehensive foundation and framework for the entire discourse. The content includes the crucial background knowledge, essential theoretical frameworks, and key concepts necessary to understand the subsequent analysis. This ensures that readers have a solid foundation in the topic before exploring more detailed and subtle elements. Furthermore, it facilitates gradual progression by preloading the background material. The arrangement promotes the gradual progression of the topic, with the initial chapters serving as a foundation By devoting more space to these initial discussions, we are able to provide a comprehensive and nuanced examination, which is crucial for a comprehensive understanding of the topic. This approach allows for a more detailed and focused exploration in subsequent chapters. This sequencing helps maintain consistency and improves the readability of the piece. In fact, this systematic approach ensures that readers are adequately prepared for subsequent chapters. In addition, it facilitates a systematic progression of ideas and promotes a coherent and compelling examination of the topic, as illustrated below.

7. Short Summary For Each Chapter

The first chapter: provides an introduction to an explanatory review of electronic banks, comparing them with conventional banks, highlighting their differences, advantages, and disadvantages. The research relies on concepts within the framework of Jordan and the international community to illustrate the variances between traditional banks and electronic banks, the personal benefits for customers and investors, and their impact on the national economy.

The Second chapter: aims to clarify the challenges facing electronic financial operations, including new and ongoing challenges related to electronic payment methods, technical and

criminal protection of electronic banking operations, and the vulnerabilities faced by banks in money laundering operations. The goal is to define the concept of challenges facing electronic banks. This chapter includes a research of the legal regulations in Jordan and the European Union, including charters, directives, and case law. Additionally, it examines the impact of international law within the framework of the Open Method of Cooperation to enhance the drafting of rules in Jordanian Transaction Law.

In addition, the exploring the impact of international law within the framework of the open cooperation method to enhance the formulation of Jordanian transaction law regulations. These regulations must strike a balance between ensuring the security and privacy of users and promoting innovation and growth in the electronic payment industry. By achieving this balance, we can create a digital financial ecosystem that is comfortable and secure, as well as flexible enough to accommodate future developments.

The third chapter: explains the government policies underlying the basic ideological concepts surrounding the subject, the introduction of security, protection, electronic financial stability, economic balance, government policies in regulating the financial banking sector, monetary policies of central banks, and considering different jurisdictions. The basic arguments for rationalization were discussed, with reference to the historical context of the emergence of such policies and doctrines, the basic model of the Jordanian Electronic Transactions Law and the applications of the Central Bank of Jordan. The importance of this part lies in revealing how different religions or ideologies affect financial stability, because these beliefs and ideologies raise the issue from different legal perspectives and economic interests. The European model and the policies of the United States Central Bank (Fed) reveal the extent to which fiscal policies can be de-liberated. Moreover, it may provide a supporting analysis of the model of the recent crisis that occurred during the coronavirus pandemic in the EU, where economic reasons justify flexible working rules. Therefore, the contribution of European and American orientation models to this research, i.e. including the concept of due process, and although both models differ significantly in theory and practice, they may serve each other in some specific paths and results. The chapter ends with the most common findings between financial security policy and the principle of customer responsibility, as appropriate, with reference to the various findings related to the challenges facing electronic banks.

The fourth chapter: also addressed the legal status of Revolut Bank - a case study, which is one of the largest and most important electronic banks currently operating in Europe, by studying it and benefiting from its distinguished experience, especially since it spread and expanded during the Corona pandemic. Its case was studied in terms of the bank's financial performance, the spread and expansion of Revolut Bank, dealing with stakeholders, how to prevent fraud and customer safety, and the greater focus on the legal regulation of the challenges facing the bank during the stages of its establishment and the rapid development of the foundations of legal regulations and instructions to ensure legal protection for electronic banking operations and to be an advanced model that can be used in Jordanian experiences in the event that electronic banks are established later.

Finally, **Fifth chapter:** includes the conclusion, results and suggestions to summarize the findings of the research.

8. Research Limits

- Researching spatial: borders in the Hashemite Kingdom of Jordan, EU and international legislation in general.
- Time limits: the research covers the time period from 2008 and during the Corona pandemic to 2024.
- Legal limits: the research deals with the Jordanian Electronic Transactions Law No. 15 of 2015, the Jordanian Banking Law, EU directives, and international laws in general with jurisdiction.
- The research's scope is defined by its focus on electronic banks, the legal regulations and legislation governing them, the challenges they encounter, and their interactions with customers, stakeholders, and central banks.

Chapter I

Definition Of Electronic Banks

The first chapter of this research deals with an illustrative review of the concept of electronic banks and their comparison with traditional banks in terms of the differences between electronic and conventional banks and the advantages and disadvantages of each. To this end, emphasis has been placed on analyzing the concepts associated with their domestic framework in Jordan and the international community to clarify the differences between the transition from traditional banks to electronic banks, the benefits to customers and investors, and their impact on the future of the national economy.

Covid-19 has accelerated executing of electronic banking services, enabling customers to easily access contactless electronic financial services at any time and from anywhere using digital platforms such as mobile applications and websites. As a result, interest in electronic banks has increased for their positive solutions for financial operations and electronic payments, which were urgently needed due to the restrictions imposed during the pandemic; however, this rapid openness led to the emergence of challenges, threats, and fraud attacks. Additionally, the theft of money and data necessitates a reassessment of the legislation governing this sector to evaluate the extent to which these regulations align with the rapid advancements in the electronic banking sector. This evaluation aims to ensure legal protection within a robust legal framework that balances the need for both acceleration and operational flexibility. In this chapter, I will define electronic banks and explore the concept of electronic banks under Jordanian laws, specifically the Jordanian Electronic Transactions Law No. 15 of 2015. Furthermore, I will compare electronic banks with conventional banks to elucidate the benefits of transitioning from traditional financial operations to electronic financial operations, and I will examine the advantages, disadvantages, and overall impact of this transition.

I.1. The Concept Of Electronic banks

Electronic banks encompass all electronic and online banking services, representing an advanced and comprehensive evolution of concepts such as remote financial services, remote electronic banking, home banking, online banking, and self-service, which originated in the early 1990s. These services are interconnected, enabling financial service customers to access their bank accounts and perform various transactions from anywhere at any time. Initially, this was facilitated through dedicated lines, but with the advent of the Internet, customers can now access services through public online connections. The concept of remote financial services relies on specific software installed on the customer's computer system. This software, available either free or for purchase, enables the execution of various banking functions remotely. Customers can obtain these software packages from their banks or purchase them from providers. Notable examples include the Microsoft Money Package and other personal financial management programs, such as personal computer banking software, which continue to be widely used in both concept and form. [3]

Interest in electronic banks has increased, as banks that do not have a physical presence (in the form of branches, except for some requirements related to public administration and complete the requirements for establishing a banking relationship, providing services and products, and implementing banking operations with their customers remotely without time or space restrictions) using Internet platforms and mobile applications from the bank's branches or any form of its presence.[4]

In the twenty-first century, banks have transitioned to providing all their services through electronic means, eliminating the need for multiple physical branches characteristic of traditional banking. The evolution of electronic banking concepts has occurred over various periods, spurred by the rise of e-commerce. Legislation must adapt swiftly to keep pace with the rapid developments in this dynamic sector. The emergence of e-commerce has had a significant

[3] Electronic Banks, Volume 1, p.1, research Nshour at the link: access on 7 may 2023 , https://ketabonline.com/ar/books/100108/read?part=1&page=1&index=4653611

[4] Central Bank of Jordan. *The Payment System in Jordan, the Sixth Annual Report for the Year 2021*. Department of Supervision and Control of the National Payment System.

impact on electronic banks, aligning them closely with the principles of digital trade. Consequently, numerous banks and financial institutions now conduct transactions via the internet, leveraging the efficiencies and conveniences offered by electronic platforms[5]. As imagined, checks can be written, money can be transferred and accounts managed without leaving your home or office, and all transactions are conducted electronically through the Internet. All the customer needs is a device connected to the Internet to access electronic banking operations. The most important administrative applications of electronic transactions that appeared in conjunction with the ICT revolution are "e-government". The e-government program in Jordan reflects the country's commitment to implementing e-transactions. Embedded within the broader context of government and digital transformation, this program constitutes a key component of the Kingdom's development initiatives and projects. Its overarching goal is to foster sustainable development and advancement across all facets of life, emphasizing the importance of leveraging technology to enhance governance, efficiency, and accessibility within governmental processes and services."[6]

In fact, banks were significantly impacted by the emergence and widespread use of the Internet. This network was effectively utilized for electronic activities, with banks playing a crucial role in revolutionizing the banking industry. By adopting the latest technologies, banks were able to enhance the speed, accuracy, and flexibility of their electronic services, thereby accelerating the provision of banking services to customers. The genesis of the notion of electronic banking was influenced by these causes [7].

Historically, liberalization from manual labor in the banking sector began at the beginning of 1971, and the transfer of services between countries became simpler and faster through inter-country money transfers (SWIFT) (Association for Universal Interbank Financial Communication).[8] The second phase commenced in early 1983, marking the advent of networking and the era of automated and electronic communications on a worldwide scale. These technologies were employed to facilitate access to the customer's residence or workplace,

[5] Kafi, Mustafa Youssef. "*Money and Electronic Banking ".* First edition. Damascus: Dar Raslan for Publishing and Distribution, 2012, p. 111.
[6] The official website of the Jordanian Ministry of Digital Economy and Entrepreneurship.
[7] Jaber Ali. *Journal of Developing Regions* 57, no. 2 (Spring 2023). p. 341-353. doi:10.1353/jda.2023.003 .
[8] The Society for Worldwide Interbank Financial Telecommunication, legally S.W.I.F.T. SC, is a Belgian banking cooperative providing services related to the execution of financial transactions and payments between limited banks worldwide

commonly referred to as "home banking". The 1990s marked a significant turning point characterized by major technological advancements, including the emergence of mobile phones and the widespread adoption of the World Wide Web. It was during this period that the electronic banking system was established, with the first electronic bank being established on October 18, 1995 [9], Net Bank in America, An internet-based bank that offers all the financial services typically given by a traditional bank, without any physical offices or headquarters.

On the other hand, the concept of a conventional bank, according to the Jordanian legislator in Article 2 of the Banking Law No. 28 of 2000, is that the bank is: "a company licensed to conduct banking business in accordance with the provisions of the Banking Law, including branches of foreign banks licensed to operate in the Kingdom." Article (6) of the Banking Law stipulates that in order to license a bank, it must be a public shareholding company, with the exception of branches of foreign banks, subsidiaries, and exempted companies. Article (93) of the Companies Law, Law No. (22) of 1997, specifies that only public shareholding companies are authorized to conduct banking operations. This restriction stems from the inherent risks associated with banking activities, necessitating guarantees for individuals investing their funds in such operations. These guarantees are typically provided by public shareholding companies. Consequently, Jordanian financial institutions are not entitled to offer these guarantees, limiting banking operations to public shareholding companies. As a result, entities like the Jordan Commercial Bank must adopt the form of a public shareholding company to engage in banking activities legally. Notably, commercial banks, which primarily focus on providing banking services, are distinct from other banks in their ability to accept deposits that are withdrawable via checks [10].

The Central Bank of Jordan serves as the regulatory authority overseeing banks and financial institutions. It operates as a public institution endowed with legal personality. In addition to its supervisory role over banks and its responsibility for implementing measures to tackle economic and financial challenges, the Central Bank also functions as the banker for the government and public institutions. Acting as a financial agent on behalf of the government and public entities,

[9] George Abu Jerais and Khashan Rashwan, "*Introduction to Internet Banking"* Beirut : Union of Arab Banks, (2004), .p.15.
[10] Al animat, Mohammad. "*Technical Protection of Electronic Banking Operations in Jordan",* Curentul Juridic 92, no. 1 (2023).p. 98.

it provides banking services. However, it's worth noting that the Central Bank does not engage in banking operations for individuals or informal entities[11]. As for specialized banks, which are banks that depend on financing industrial, agricultural or commercial economic projects or operations, and depend for their resources on the state budget allocated to them, they do not carry out banking operations. It is subject to the provisions of the Banking Law, an example of which in Jordan is the Cities and Villages Development Bank, established by Law No. (63).

The Jordanian legislator has dealt with the issue of electronic operations in article 22 of the Jordanian Electronic Transactions Law [12]. Article (22/1/A) of the Jordanian Electronic Transactions Law stipulates the following: "Subject to the law, every payment and electronic transfer company of funds shall obtain a license from the Central Bank of Jordan."

The Jordanian legislator has entrusted the Central Bank of Jordan with the oversight and regulation of financial companies, rather than delegating these responsibilities to the Ministry of Digital Economy and Entrepreneurship or the Jordanian Ministry of Industry and Trade. Licensing, administrative procedures, and supervisory functions are under the purview of the Central Bank, which imposes specific conditions for obtaining licenses.

It is considered one of the most important strategic steps taken by the Jordanian legislator to give full powers to the Central Bank as a decision-maker to take the right steps and issue regulatory instructions and decisions that suit digital development and the development of banking services, including electronic banks, and confirms that one of the important **hypotheses** on which this research was built, which assumes; "Are there Regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system".

This indicates the great awareness and understanding by the Jordanian legislator of the importance of not restricting and giving the competent authorities (the Central Bank of Jordan) the opportunity to move forward towards digital leadership to open the door to digital investments through electronic banks, because this sector needs to keep pace with the rapid pace

[11] Ali Salman Saleh and Rami Zeitoun. "Islamic Banks in Jordan: Performance and Efficiency Analysis" *Islamic Economics Review* 11, no. 1 (2007).p. 49.
[12] Jordanian Transactions Law No. 15 of 2015.

of financial technology due to the loss of benefit and great harm that may occur due to any legislative shortcomings and gaps that delay this rapidly growing sector.

E-banks may operate independently on the Internet, allowing users to access financial services typically provided by traditional banks. The concept of the electronic bank encompasses all electronic transactions conducted by banks or financial institutions via the Internet, spanning from the promotion of banking services to their execution and operation. Indeed, some financial companies and economic entities possess advanced capabilities to manage financial websites offering services comparable to traditional banks. These entities can establish specialized banking rules and provide facilities to customers, thereby expanding their scope beyond their original foundations.[13] This raises significant controversy and disagreement regarding the classification of these entities as banks solely based on their engagement in banking activities. If they are indeed deemed as banks, they would be subject to the same regulatory provisions as traditional banks, including rules and procedures for supervision by banking authorities such as central banks.

A question may be asked, did the Jordanian legislator in this law distinguish between the concept of electronic banks and financial companies banking via the Internet, and does this text cover the absolute concept of electronic banking, or is the electronic bank what is meant by this text of the article?

In fact, the electronic company is a term that differs from the electronic bank, and this will be answered through the text of the article of the Jordanian Electronic Transactions Law No. 22/C) that states the following: "For the purpose of this article, the electronic payment and transfer company for funds means the company that practices payment, transfer or electronic financial settlement services or the issuance and management of electronic payment tools and systems in accordance with the provisions of this law and the regulations and instructions issued pursuant thereto and other relevant legislation" and here we note that the concept of the electronic company, as defined by the Jordanian legislator is different from the concept of the bank, and that appeared clearly in the sense in which the text of the previous article was mentioned. It appears that the Jordanian legislator did not explicitly mention or define the concept of

[13] See Arab, Younis, "*Electronic Banks between Advantages and Disadvantages",* Alexandria: Dar Al-Fikr Al-Jamia, (2005).p. 12.

electronic banks in the context of the law. As such, it can be inferred that the legislation primarily focuses on companies engaged in electronic payment and financial transfer services, rather than electronic banks. Consequently, there is a distinction between the two concepts, indicating that the law does not encompass regulations specific to electronic banks.

The concept of electronic banks extends beyond a mere formal framework; it encompasses an objective framework as well. Merely mentioning the services that a bank can provide without actual transaction capabilities does not fully capture the essence of electronic banking. Electronic banking involves more than just having an online presence and complying with advanced technology requirements. With the advent of the Internet, electronic banking has made significant strides in the banking sector, leading to the emergence of fully electronic banks operating solely online. These electronic banks offer a wide range of financial services and banking advice tailored to meet customer needs. The interaction between customers and electronic banks occurs through dedicated programs provided by the bank, allowing customers to engage with banking services anytime and anywhere using their devices.[14].

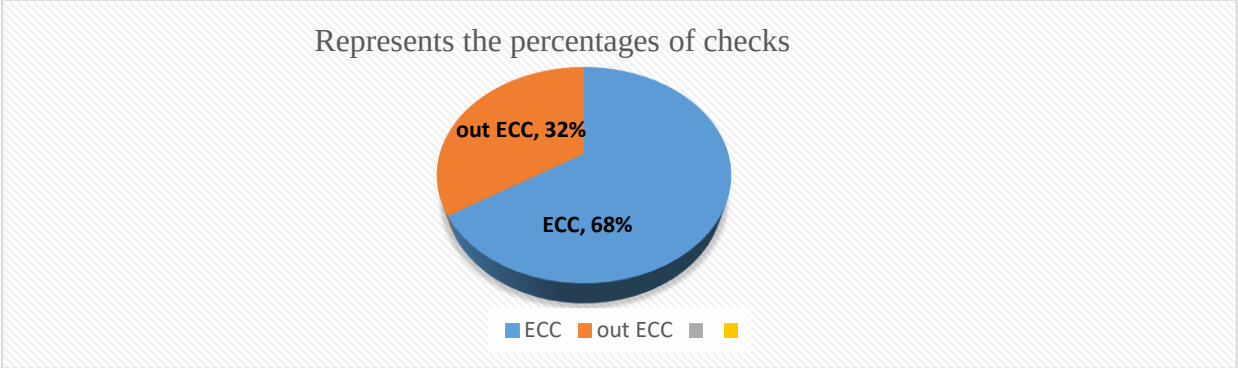
Some researchers have known that electronic banks are "banks that have a full presence on the Internet, and their website contains all the necessary software for banking business [15], as this bank provides its services to the customer by conducting all financial transactions related to the bank through any site in it, through a line provided by the bank, which allows him to carry out all his transactions without the need to go to the bank's management or the so-called bank office." [16]

On the other hand, the United States of America is a leading country in the world in the field of technological development and the provision of electronic services via the Internet, and its Internet banks are among the most active electronic banks. In general, there is a delay in licensing electronic banks to provide services online[17], and this is due to the lack of e-commerce in the region significantly, as is the case in some Arab countries, and a number of reasons can be summarized, which are the limited spread of the Internet in remote places, and the lack of

[14] Bilal Abdul Muttalib Badawi, "*Electronic Banks*, 1st ed. (Cairo: Dar Al-Nahda Al-Arabiya, 2006) p. 8.
[15] Arab, Younis, Electronic Banks between Advantages and Disadvantages, Kenana Information Technology Company, Jordan, www.kenanah.com , accessed on 27/5/2022.
[16] Mounir Janabihi et al., Electronic Banks, 1st ed. (Alexandria: Dar Al-Fikr Al-Jamia, 2005), 10
[17] According to the analysis of Abdel Fattah Mourad, president of the Supreme Court of Appeal in Alexandria.

knowledgeable people with the importance of this type of service, the lack of incentives to encourage customers, the ease of electronic hacking and sabotage of financial data, psychological and cultural barriers and mistrust. In the same context, electronic services were launched in Jordan in 1998 through Petra Bank, in a simple way such as revealing the balances of accounts, deposits, loans, electronic credit cards and money transfers, and the beginning of electronic operations was the broadest beginning after the Central Bank of Jordan approved the drafting of the Temporary Electronic Transactions Law No. 85/2001[18], as amended by Law No. (15) of 2015.

Figure No. (1): Represents the ratios of cheques executed through the electronic cheque clearing system against cheques executed outside the electronic clearing system 2021.[19]



Source: Jordan's National Payments System Report 2021 issued by the Central Bank of Jordan

It becomes clear to us through Figure No. (1) that electronic banking operations in Jordan are proceeding in an accelerated and sophisticated manner and there is a demand for it by citizens, merchants, and customers, so we note that the operations that take place through the clearing of electronic checks are very high, up to 68% in 2021, on the other hand, the operations of clearing checks outside the electronic clearing system is 32%, meaning that the operations of electronic checks within the clearing system are twice as weak as operations outside the electronic purposes system, and this indicates that there is a great demand for Electronic financial operations through traditional banks, meaning that customers have become preferred and seek electronic operations instead of traditional operations, and this is an incentive for decision-

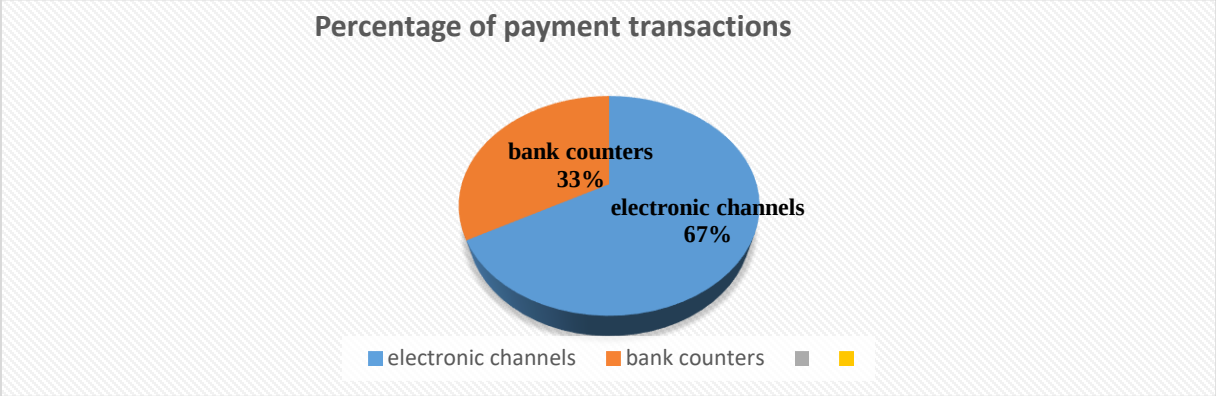
[18] Jordanian Electronic Transactions Law No. 85/2001 published in the Official Gazette on 31/12/2001) As amended by Law No. 15 of 2015.
[19] Jordan's National Payments System Report 2021 issued by the Central Bank of Jordan.

makers and legislators to review the Electronic Transactions Law in terms of content to include electronic banks within its regulations.

Jordanian banks are still working on developing and modernizing electronic payment channels and making them available to customers as the main and best option for customer service by reducing the operational cost incurred by the bank. At the customer level, services are obtained.

This will contribute significantly to enhancing financial commitment in the Kingdom, which is what the Central Bank of Jordan should aim to achieve.

Figure No. (2): Percentage of payments executed through bank counters and channels electronic to the total electronic and non-electronic transactions in 2021.[20]



Source: Jordan's National Payments System Report 2021 issued by the Central Bank of Jordan.

The analyzing: Figure No. (2) reveals that electronic financial transactions constituted 67% of the total financial movements in 2021, compared to 33% for non-electronic financial movements. This significant percentage highlights the growing preference and need for development in the electronic banking sector, which is rapidly expanding. This trend serves as an important indicator for decision-makers to take positive steps and focus on advancing electronic banking operations. The shift towards electronic transactions surpassing traditional financial operations in 2021 may have been significantly influenced by the COVID-19 pandemic, which accelerated the adoption of digital exchanges. This trend underscores the practical importance of this research. Consequently, there is a need to compare and contrast traditional banks with electronic banks to understand the benefits and drawbacks of transitioning

[20] Jordan's National Payments System Report 2021 issued by the Central Bank of Jordan.

from a traditional to a electronic banking environment. This analysis will help elucidate the advantages and disadvantages associated with the evolving electronic banking system.

In the same context, the popularity of electronic payments has increased in recent years due to their convenience and speed. Electronic payment methods include credit/debit cards, online bank transfers, mobile payments, and digital wallets, and we note the superiority of electronic payment methods in cash, checks, and electronic money transfers.

According to an account conducted by 2021-compliant Clay Payments, electronic payments accounted for 73% of non-alternative merchants globally in 2020, up 65% in 2015. This trend is a foregone conclusion, with electronic payments looking for almost 78% of all cashless trade by 2025.

I. 1.1. Electronic Business Papers

As is known, the Internet has become a fundamental pillar for providing banking services and transactions. Innovations in banking have transitioned traditional services to electronic formats, significantly reducing material costs and effort for both customers and banks. Conventional banks have also incorporated electronic financial transactions, such as bill payments and fee payment services, which, while similar in function to traditional transactions, are conducted electronically for convenience and efficiency. Electronic banking operations involve offering both traditional and innovative banking services through electronic communication networks. Banks and financial institutions providing these services offer detailed information about the services available. Customers benefit from these electronic services by accessing and managing their transactions, checking account balances, updating personal data, requesting loans, and performing banking operations such as money transfers. This transformation has not only streamlined financial processes but also enhanced accessibility and efficiency for users[21]. The most important electronic banking transactions will be presented, namely;electronic commercial

[21] Mahmoud Ahmed Ibrahim Al-Sharqawi, "The Concept of Electronic Banking and its Most Important Applications," in *Conference on Electronic Banking between Sharia and Law*, United Arab Emirates University, 2003, pp. 17-18. & Nazzal Salim Barham, *Provisions of E-Commerce Contracts*, 1st ed. (Dar Al-Thaqafa, 2009), p. 169.

papers, electronic documentary credits, electronic bank transfers, and electronic money. These banking transactions, credit payment cards, will be briefly discussed in Chapter II.

Electronic commercial papers include the electronic bill of exchange and the electronic check.[22] The electronic bill of exchange is equivalent to its paper counterpart, containing all the legally required data. The main difference is that the drawer issues it electronically, and the bank processes it via computer. Similarly, the electronic check mirrors the paper check in all essential details. The drawer completes the check information on a computer screen, signs it electronically, and sends it to the beneficiary online. The beneficiary then signs it electronically to obtain the check number, which is subsequently deposited into a bank account.[23]

I. 1.2. Electronic Documentary Credit

A documentary credit is a legally binding written commitment issued by a bank to the customer, authorizing the payment or acceptance of documentary bills of exchange drawn on the customer by a third party in the beneficiary's country. This payment is made against specific documents specified by the beneficiary. Electronic documentary credits refer to the exchange of documents and records electronically through email or electronic platforms. [24]

I. 1.3. Electronic Bank Transfer

Electronic bank transfer from one account to another, or to another beneficiary, is a transfer that is made electronically between banks and financial institutions, and orders and documents are sent in this form. The customer can make an electronic transfer from one account to another through an ATM, as this service is available in most banks[25], according to the text of Article (26) of the Jordanian Electronic Transactions Law. Instructions for electronic transfer operations for the year 2005 were issued based on electronic transfer and in accordance with Law No. (85) of 2001, and Electronic transfer operations in (18) articles, and Article (2/a) of these instructions states that electronic transfers include any electronic means that the customer and the bank agree to use, including but not limited to, electronic transfer units, deposits, direct withdrawal of funds

[22] Bilal Abdul Muttalib Badawi, *Electronic Banks*, 1st ed. (Cairo: Dar Al-Nahda Al-Arabiya, 2006), 1961.
[23] Ibid., p. 1962.
[24] Hussein Shehadeh Al-Hussein, *Electronic Banking Operations*, in *Banking Conference*, Faculty of Law, University of Beirut, 2002, p. 201.
[25] For more details on electronic bank transfer, see Bilal Abdul Muttalib Badawi, *Electronic Banks*, 1st ed. (Cairo: Dar Al-Nahda Al-Arabiya, 2006), pp. 1964-1966.

through ATMs, transfers by phone, transfers originating through credit card transactions, and transfers originating via the Internet.

I. 1.4. Electronic Money

Electronic money is one of the means of commercial transactions over the Internet, it is similar to paper money and metal in most of its characteristics, except that it is electronic and intangible, in the form of electronic units that are stored on the computer in an electronic wallet. These units can be used in commercial transactions[26]. Purchases are made online and payments are conducted using electronic units. Payment can be made with electronic money in one of two ways. In the first method, the customer maintains two accounts: one in regular currency and one in electronic currency. The customer transfers a certain amount from the regular currency account to the electronic currency account. Subsequently, transactions are completed using the electronic currency. In order for the customer to be able to pay by electronic money, the seller must have two bank accounts with the same bank, one in regular currency and the other in electronic currency. Payment is made by asking the bank to record the value paid to him in the account in electronic currency. Concerning the second method, payment is made using electronic money for this purpose, so the value of these cards is stored inside them, and there is no need for users of these cards to access the Internet through pre-prepared cards, as they are electronic money outside the network, and this card carries data that includes the name of its holder, card number, account, expiration date and the name of the entity that issued it, as the card is passed on a device located in specially prepared stores. The purpose of this process is to ensure the validity of the card as a means of payment, and to issue a receipt in three copies: the customer signs a letter, which the commercial store sends to the payment services company to pay him the value of these receipts.

On the other hand, both commercial and investment banks must have robust cybersecurity protocols to safeguard against cyberattacks and oversee financial markets. Both conventional and electronic banks involved in financial market operations and trading must adhere to supplementary requirements, such as the Markets in Financial Instruments Directive. MIFID II,

[26] Mahmoud Ahmed Ibrahim Al-Sharqawi, "The Concept of Electronic Banking and its Most Important Applications," in *Conference on Electronic Banking between Sharia and Law*, United Arab Emirates University, 2003, p. 29. & Ahmed Safar, *Electronic Payment Systems*, 1st ed. (Al-Halabi Legal Publications, Lebanon, 2008), p. 24.

EU [27] Legislators have endeavored to require banks of all kinds to issue compulsory regulatory measures, Banks send reports to authorities in order to maintain openness and adherence to rules. Electronic banks frequently encounter regulatory obstacles that are interconnected with technology, cybersecurity, and online services, as a result of the substantial and swift advancements in the realm of financial information technology. Nevertheless, the fundamental regulatory principles are relevant to both conventional and electronic banking operations in (EU), with the objective of safeguarding the stability and integrity of the financial system, as well as the interests of consumers and investors.

It is considered one of the most important strategic steps taken by the European legislator to give the European Central Bank powers commensurate with taking the right steps and issuing instructions and regulatory decisions that suit digital development and the development of banking services, including electronic banks. confirms that one of the important **hypotheses** on which this research was based is that "International coordination and cooperation between regulators is needed for the proper international management of electronic banks, which may lead to a combination of legislative regulations; and different jurisdictions to adapt and define appropriate jurisdiction and criteria for disputes involving e-banks." This indicates the great awareness and understanding by the European legislator of the importance of not restricting and giving the competent authorities (the European Central Bank) the opportunity to move forward towards digital leadership to open the door to digital investments through electronic banks, because this sector needs to keep pace with the rapid pace of financial technology due to the loss of interest and the great damage that may occur due to any legislative shortcomings and loopholes that delay this rapidly growing sector, and this has appeared in particular, the promotion of the smooth operation of payment systems, the contribution to the smooth conduct

[27] MIFID II is the abbreviation for the second "Markets Directive in Financial Instruments". The European Union (EU) introduced the regulatory framework on 3 January 2018. MIFID II is a significant modification of the initial MIFID, implemented in 2007, with the aim of enhancing the transparency, efficiency, and dependability of the financial markets in the European Union. The primary goals of the mandate are to foster market integrity and safeguard investors. MIFID II is a comprehensive and extensive regulatory framework that applies to the financial industry of the European Union. The standards provide market transparency and safeguard investor interests, compelling financial institutions and market participants to comply with them. Non-European Union (EU) enterprises who provide services to consumers in the EU are likewise impacted by MIFID II, laws and are required to adhere to them.

of policies pursued by competent authorities relating to the stability of the financial market system. [28]

From another perspective, The European Central Bank (ECB) collaborates with multiple regulatory bodies and organizations within the European Union (EU) to ensure legal regulation of electronic banks. The ECB and the European Banking Authority (EBA) maintain a strong partnership, as the EBA is a crucial regulatory body in the EU.

that oversees banking regulation and supervision.[29] This agreement establishes technical standards and suggestions that promote consistent execution of EU financial rules, especially provisions related to electronic banking. Furthermore, it plays a role in aligning regulatory plans among EU Member States and serves as a vital authority for regulation and oversight. Furthermore, the ECB has the capacity to cooperate with other regulatory entities and organizations to tackle specific challenges in the financial sector through joint initiatives. These initiatives may encompass subjects such as cybersecurity, digital innovation, or cross-border payment systems, all of which are interconnected with e-banking [30].

I. 2. Electronic Banks And Conventional Banks

Covid-19 has strengthened the shift towards electronic banks and digital financial operations, and the shift towards financial digitization is increasing day by day because of its benefits such as easy and fast access, saving time and effort and reducing costs. In short, moving to the environment for digital financial operations can achieve many of the advantages that customers and investors alike need, and the pandemic was the main driver of excessive digital use, which encouraged many individuals and companies to shift and use electronic banks due to closures and limited travel; airlines were suspended and borders between countries were closed.

Electronic banks have gained significant prominence in the banking sector, particularly in recent years, due to their global proliferation and rapid adoption rate. These banks offer customers the

[28] Opinion Of The European Central Bank of 11 April 2022 on a proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (CON/2022/14).
[29] Mohammad Elayan Al-animat, *Legal Perspectives and Discrimination of Electronic and Conventional Banks*, *Lex et Scientia International Journal*, 2023, p. 154.
[30] European Central Bank, "Study on Consumer Payment Positions in the Eurozone (SPACE)," 2022.

capability to issue instructions and perform financial transactions 24/7 from any location worldwide. The procedures are documented by the bank and subsequently referred to the relevant authorities for electronic execution, highlighting the substantial value provided by electronic banking services. Electronic banks impose financial fees on consumers, clients, and other banks; however, the cost of electronic transactions is relatively low compared to traditional banking transactions.[31]

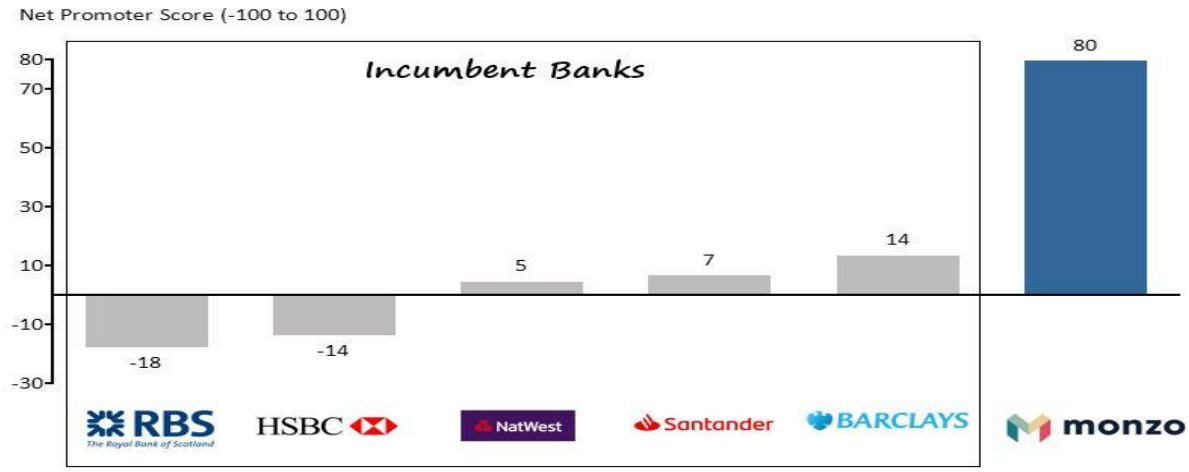
It is noteworthy that a single website can replace numerous branches that traditional banks would need in each city, significantly reducing the financial costs associated with traditional banking. Unlike traditional banks, which incur expenses for building maintenance and periodic repairs, electronic banks avoid these financial burdens. The substantial credit goes to the technology infrastructure, particularly computers, which replace many employees, thereby lowering operational costs for electronic banks.

However, e-banks are quickly becoming popular due to their creative range of products and easy-to-use mobile applications. Customers that prioritize convenience and do not need face-to-face interactions with bankers are increasingly using e-banking. Customers may also take advantage of the lower expenses and better interest rates provided by online banks for their financial deposits.

By critically reviewing one of the European e-banking experiences through a report attributed to Monzo Bank Ltd and as shown in Figures (3&4) below, UK-based e-bank, which presents innovation and transformational changes in the bank, the prevailing innovation process in the bank in light of the concepts And theories related to other banks to clarify the ratios through comparison with traditional banks.

Figures No. (3&4) A review of one of the most important European electronic banking experiences through a report attributed to Monzo Bank Limited, how customer interest in electronic banks increased, especially during the beginning of the Corona pandemic (2020).

[31] Cedric J. Magnin, *The Telephone Banking Contract in Swiss International and Comparative Law*, ILSA, 2001, p. 32.



Source: Monzo Bank official website [32].

We notice in Figure No. (3) an increase in the number of customers in the year 2019 and up to the year 2020, with an increase of 2.3 million customers, and this is considered a large number. In the same year, we notice in the previous figure an increase in the amount of financial revenues that entered Monzo Bank Ltd, amounting to £ 47.5 million over the previous year. In the same context, we notice figure No. (3) Customers' financial deposits have increased noticeably and clearly from 2019 to 2020, with an annual increase estimated at £930.7 million. This confirms that electronic banks have become widespread and more accepted by customers; this confirms the need for this sector to spread, expand, regulate and protect, one of the challenges faced in this sector.

[32] Available at; https://monzo.com/ access on 7 March, 2024.

In the same context and with regard to figure No. (4) the creators of the NPS [33], promoter score, An NPS score over 0 is acceptable, above 20 is fantastic, and above 50 is exceptional, according to Bain & Company. Higher than 80 is top percentile. Note that a high NPS score relies on whether you use absolute or relative NPS, Over 70 NPS shows your consumers adore you and your firm is getting good word-of-mouth from recommendations. The better your NPS, the more likely client recommendations will become new leads and money for your organization, from the above indicates the importance of electronic banks, we note that Monoz Bank has recorded a large number compared to the traditional banks currently existing in the same country UK, and this indicates the spread and great desire among customers to move towards electronic banks, which confirms the importance of the research that we are doing and the importance of this topic in our current time.

The global financial landscape is undergoing a rapid transformation, with electronic payment methods becoming increasingly predominant. As cash and traditional payment systems gradually yield to digital alternatives, the convenience and efficiency offered by electronic payments have revolutionized financial transactions. Nonetheless, this digital shift presents its own set of challenges. Electronic payment methods bring with them a new set of risks for both consumers and businesses, and these risks require comprehensive legal regulation.[34]

This is what may prompt customers and stakeholders to think long and hesitate to invest in electronic banks, which requires legislators to find a legal regulation that limits these risks, which will be answered and many of them will be reviewed in the following chapters, which face electronic banking operations and the most important operations carried out by the electronic bank and how the regulatory authorities deal with this threat.

This is what the **third sub-question** of the research question focuses on, which is the challenges facing electronic banks and the risks. What are these challenges and how can these challenges be overcome and protected within the framework of conservation and protecting this sector from violations through a large set of instructions, regulations and laws that ultimately lead to

[33] Net Promoter Score® (NPS®) is a common metric for evaluating customer experience (CX) and loyalty. It measures customers' satisfaction with a company and their willingness to recommend it to others.
[34] R. Zhang, "Factors Affecting Consumers' Mobile Payment Behavior: A Meta-Analysis," *Electronic Commerce* (2019):18.

protecting this sector from any violation and any cyber risks it may face and protecting customers as well.

In general, "the decision between a traditional and electronic bank will be influenced by personal preferences and banking requirements. Traditional banks may be preferred by some customers who value physical presence, personal service, and established brand familiarity".[35]On the other hand, customers who appreciate convenience, minimal costs and creative product offerings can opt for e-banks, preferably familiarizing themselves with e-banking services, costs and security measures before opening an account, regardless of the type of customer accounts.[36] Traditional banks are considered to have physical locations where customers can stop and interact with a cashier or customer support agent to provide traditional financial services. On the other hand, the internet or mobile applications can be used to access e-banks.

As is known, electronic banks are recognized for their ability to conduct operations for their electronic financial customers whenever and wherever they choose, unlike traditional banks that are only available during normal working hours and have limited working hours, with the ability to view accounts and complete some transactions online or through mobile applications, in return electronic banks provide a high level of convenience to their customers. As a result, customers can do banking whenever and wherever they choose to process.[37]

Consumers may pick an electronic bank over a traditional bank for convenience. Most consumers bank outside of banks in a fast-paced atmosphere. This has helped e-banks offer user-friendly apps and websites that let customers check their accounts and make transactions anywhere,[38] and anytime" It is important to keep in mind, however, that some customers may still enjoy the personal interaction and personal touch of a local bank branch. Traditional banks

[35] SD, Kavitha Vanni. "Electronic banking Units: Visualize and Accept Customers in Rural India." *IUP Journal of Bank Management* 21, no. 4 (November 2022), pp. 7-26.
[36] Bloomberg. "Banks Close Branches at Record Pace as Electronic banking Booms Arrive." 2021. access Apr 10, 2023, https://cutt.us/6YFY5
[37]Since the onset of the COVID-19 pandemic, there has been a substantial rise in the utilization of mobile banking applications, as indicated by a 2021 J.D. Power report. The research revealed that a significant proportion of retail bank clients, specifically 38%, utilize mobile banking applications to oversee their accounts, in contrast to the 29% recorded in 2019. Additionally, the research revealed that clients who utilize mobile banking applications exhibit higher levels of satisfaction with their banks' services compared to those who do not. Origin: J.D. Power. "2021 U.S. Retail Banking Satisfaction Study".
[38] In 2020, 57% of U.S. people managed their accounts via mobile banking applications, up from 49% in 2019. Mobile banking applications are used by 79% of millennials and 70% of Gen X, according to the report. From Bankrate (2020). Bankrate survey: COVID-19 boosts mobile banking.

can also provide other services that are difficult to obtain through an electronic bank, such as financial advice or notary (legal clerk) services. In general, convenience is taken into account when choosing between a traditional bank and an electronic bank and customers prefer to consider the advantages of being able to conduct their banking transactions at any time and from anywhere against the potential disadvantages of not being able to visit a real bank branch or help customers in person".[39]

Costs and fees have always been one of the most important factors that the customer cares about, and as it is known, traditional banks require higher fees for services such as ATM fees, monthly maintenance fees, and overdraft fees. In addition, when comparing interest rates with traditional banks, e-banks may provide higher interest rates on savings accounts and current accounts. This is because E-banks do not have as many overhead costs as traditional banks, such as rent for real estate and utilities that are usually in more vibrant areas, which represent high costs that burden traditional banks in addition to the wages of employees. Traditional banks, on the other hand, often offer personalized customer service, which may benefit customers who prefer face-to-face meetings[40]. E-banks typically offer customer service through email, chat, or phone, which, while less personal, is more efficient. Both traditional and electronic banks implement and impose security measures to "protect customer personal and financial information. To counter fraud and identity theft, e-banks may offer enhanced security measures such as two-factor authentication and biometric login. Moreover, some transactions, such as ATM withdrawals or online transfers, may have lower transaction limits with traditional banks, while e-banks may impose more restrictions or no restrictions at all on some transactions; however, traditional banks may offer a wider range of account options, such as savings, verification and investment accounts. Although there are lower possibilities for an account with e-banks, they may offer unique benefits such as cashback or higher interest rates" [41]. For lending services to customers and businesses, alternatives to lending traditional banks often offer other lending options, such as mortgages, car loans, and personal loans. E-banks may offer fewer lending options or may partner with other financial institutions to provide loan services.

[39] Salahuddin Hamad Salahuddin. "Northern Oasis." *Mg.* 3 (December 2012), pp. 36-39.
[40] Ibid, p. 38.
[41] Abdullah Musa Alqam. "Money and Economy." *A* 63 (June 2010), pp. 47-48.

As is well known, e-banks heavily rely on technology, which can be a "double-edged sword." On one hand, technological advancements allow e-banks to offer faster and more efficient services. On the other hand, technology can introduce issues such as system failures or cybersecurity threats[42]; this is what the **one of hypothesis's** of the research focused on, which states: "Regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system."

As is well known, traditional banks have been operating for decades, and this has led to gaining a reputation and fame in the firm has been established for a significant duration and has successfully cultivated a reputation and brand awareness among its clientele. Customers who have engaged in direct communication with bankers are allowed to be physically present at the bank. Regarding insurance, conventional banks are often insured by the Federal Deposit Insurance Corporation (FDIC) or the National Credit Union (NCUA) management, providing [43] more security and confidence to customers that establishes the idea of security. Financial stability for customers and companies that deal with traditional banks, but at the same time Electronic banks are now in their nascent phase and may not possess the same level of trust and recognition as conventional banks.[44]

It is unwise to claim that electronic banks are still in their nascent stages and lack the same level of familiarity and trust as traditional banks. Customers may hesitate to trust a bank they cannot physically visit and may have concerns about the security of online transactions. However, many e-banks are insured by the Federal Deposit Insurance Corporation (FDIC), providing customers with some peace of mind and helping to build trust and establish a reputation. "Additionally,

---

[42] Rayan Osman. "The Reality of Electronic Banking Services in the Arab World." *International Journal of Economic Performance* 2019, vol. 2019, pp.7-26.

[43] The Federal Deposit Insurance Corporation (FDIC) is a government agency that provides insurance for deposits made by individuals and businesses in banks and savings associations. Amidst the Great Depression, a significant number of Americans experienced the unfortunate loss of their accumulated funds due to the collapse of their financial institutions. In order to prevent a recurrence of such events, the Federal Deposit Insurance Corporation (FDIC) was established by Congress in 1933. Its purpose was to ensure the stability and instill public trust in the nation's financial system. The user did not provide any text. NCUA stands for the National Credit Union Administration. It is a federal agency in the United States that regulates and supervises credit unions. NCUA is an autonomous organization responsible for supervising the National Credit Union Share Insurance Fund (NCUSIF). This insurance fund, supported by the U.S. government, provides protection for the deposits of members at credit unions that are insured by the federal government. Deposits made at credit unions that are federally chartered are guaranteed by the NCUA without the need for any further action.

[44] Mohamed Salah Mufti. "Electronic Banking." *Finance and Economics* Vol. 2013, 2013. pp. 36-38.

many e-banks offer excellent customer service and user-friendly apps or websites. It may also provide unique features such as high-interest savings accounts or fee-free checking accounts to entice customers. The reputation and awareness of e-banks is expected to grow as they become more popular and widespread " [45]

Similarly, "traditional and electronic banks' track record in terms of customer care and handling customer complaints is one element that may affect their reputation. Traditional banks may have a larger customer base and receive more complaints, but they also have greater knowledge and resources to successfully manage such issues. In contrast, e-banks have a smaller number of customer service staff who struggle to keep up with consumer demands at peak hours. Traditional banks offer a wide range of services, such as investment services or small business loans, which may allow them to position themselves as the best one for some customer categories of those banks that operate online".[46]

However, they may possess greater expertise in specific services, such as online savings accounts or mobile payment solutions, rendering them more appealing to particular consumer segments. Moreover, both conventional and electronic banks might experience harm to their reputation due to data breaches or other security concerns. Customers are becoming more apprehensive about the security of their personal and financial data, and a major breach may greatly harm the bank's standing. E-banks may face unique dangers as a result of their dependence on technology and online transactions. As to a 2021 Forbes article, e-banks are gaining popularity because of their convenience and affordability. According to a poll conducted by PricewaterhouseCoopers, 46% of consumers are contemplating only using online banks. E-banks are making significant investments in user-friendly smartphone applications and other digital service applications [47].

[45] Heba Al-Atrash and Mohamed Belhassen. "Factors Affecting the Adoption of Electronic Banking Services: A Quantitative Study of a Sample of Algerian Bank Customers." *Journal of the Institute of Economic Sciences* MG. 24, 2021. pp. 167-185.

[46] Sahar Ayman Al-Hujaila and Khaled Abu Al-Ghanim. "The Impact of E-Governance on the Reputation of Jordanian Islamic Banks." *Amman Arab University Journal for Research: Administrative Research Series* 7, no. 2 (2022), pp. 9-33.

[47] Forbes is a notable American media publishing organization, with its flagship publication being Forbes magazine, widely regarded as a top-tier journal globally. Implement strategies to effectively entice clients to get financial services.

However, the bank's reputation, whether it be in conventional or electronic form, can be influenced by factors such as customer service, product offers, and security breaches. With the increasing use of online banking, the image of e-banks is anticipated to enhance. However, it is important for these institutions to uphold exceptional customer service and stringent security measures to sustain this confidence.

Traditional banks may have an advantage in providing a wider range of account and loan capabilities. They may also have greater resources to deal with customer service questions and concerns, while e-banks are more creative in terms of product offerings and user experience. In general, the choice between traditional and electronic banks will be influenced by individual preferences and financial needs. Customers who value physical locations, personal relationships with bankers, and a wider range of services may prefer traditional banks. Conversely, those who prioritize convenience, low fees, and high interest rates may favor e-banks. Before opening an account with any bank, it is essential to carefully research the bank's services, fees, and security measures. Both traditional and electronic banks are subject to government regulatory control. However, given the relatively young industry and the potential for cyberattacks, electronic banks may be subject to greater scrutiny[48].

Before delving into the analysis of electronic banks operating globally, it's crucial to address the underlying motivation behind the loss of confidence in traditional banks. The 2008 financial crisis, played a significant role in eroding consumer trust in traditional banks, reducing their competitiveness, profitability, and prompting many business owners to seek alternative technological solutions offered by non-traditional financial institutions; based on the analysis above, the researcher posits that both traditional and electronic banks exhibit distinct advantages and disadvantages. Traditional banks excel in providing personal connections and often boast established trustworthiness, while e-banks offer superior flexibility, convenience, cost-effectiveness, and higher interest rates. The choice between the two hinges on individual banking preferences and needs, as factors such as access, convenience, costs, interest rates, customer service, security measures, transaction restrictions, account options, loan alternatives, technology integration, reputation, and regulatory oversight vary significantly between

[48] Mohamed Belhassen and Hala Tarsh. "Factors Affecting the Use of Electronic Banks by Algerian Bank Customers: An Empirical Study." *Knowledge Collections* Vol. 6, no. 1 (2020), pp. 290-306.

traditional and electronic banks. Consequently, depending on the specific banking needs of customers, one type of bank may prove more suitable than the other.

Another significant differentiation lies in regulatory oversight, as both traditional and electronic banks are governed by government laws. However, e-banks may encounter an increasing potential for cyber risks. Regulatory oversight of e-banks is imperative for safeguarding the integrity of the banking industry. While e-banks are generally subjected to similar regulations as traditional banks, their online business model inherently exposes them to heightened risks, necessitating greater scrutiny. Cyberattacks represent one of the most severe risks to electronic banking[49]. In terms of securing consumer data and preventing illegal access to their systems, it is essential that e-banks have strong cybersecurity measures. Regulatory authorities play a crucial role in ensuring that e-banks meet cybersecurity standards and are prepared to deal with any cyber risks that may arise. It is essential that anti-money/KYC requirements apply to e-banks as well, to prevent their exploitation for illegal purposes such as money laundering and terrorist financing pose significant challenges to the financial **sector.** Banks are required to implement robust systems and processes for customer identification, verification, transaction monitoring, and reporting suspicious activities to regulatory authorities. Based on these responsibilities, I contend that electronic banks should conform to laws that safeguard consumers, keep sufficient capital and liquidity reserves, preserve privacy standards, and comply with applicable international laws. Although these standards may add complexity to the regulatory compliance environment for e-banks, they are crucial for safeguarding the integrity and stability of the financial system.

Therefore, it is essential to have regulatory monitoring in place to guarantee that e-banks comply with relevant laws and regulations and maintain the confidence of the public. In order to safeguard the financial data of their clients, electronic banks must establish a tight collaboration with regulatory bodies to comprehend and adhere to the expanding regulatory framework. Additionally, they must allocate resources towards implementing advanced security measures and compliance systems.

Electronic this phenomenon also confirms my **hypothesis**" E-banks will face difficulties in complying with several financial rules, such as anti-money laundering (AML) and know-your-

[49] Muhammad Zaidan & Muhammad Hammo. "*Economic Insights*." *A* 8 (June 2015), pp. 161-181.

customer requirements, and the need to develop comprehensive strategies to manage their transaction scenarios. "

The shift towards electronic banking services within traditional banks has significantly influenced the emergence of independent electronic banks. For instance, electronic banking facilitated the introduction of digital savings accounts and enabled profits through electronic wallets. Moreover, various companies now offer customer services for electronic payment operations, including online transfers and deposits. It is worth noting that without these electronic transactions facilitated by traditional banks, the landscape would have been vastly different, with processes becoming more complex and sluggish.[50]

The researcher contends that the development of legislation to regulate electronic banks is an unavoidable necessity given the escalating challenges in this rapidly expanding sector. The proliferation of electronic transactions on the Internet, which forms the foundation of electronic banks, has led to the surge in their numbers. Electronic banks are not merely an evolved version of traditional banks; rather, they represent a novel amalgamation of advanced and systematic banking practices characterized by speed and precision. Governments must facilitate essential processes to foster the growth of electronic banks and online transactions.

I.3. Jordanian Banking System with EU & Global Integration, connectivity and Compliance.

The reader may wonder why I'm comparing Jordanian regulation to European legislation and why I am using EU legislation as a benchmark, even though Jordan is not a member of the EU. This is a legitimate question and may even be in line with the rationale that can be justified by emphasizing the impact of EU regulation on global legal and regulatory systems, especially in neighboring regions.

Although Jordan is not a member of the EU legislation serves as a widely recognized benchmark for regulatory frameworks in various areas, such as trade, human rights, environmental policy,

[50] Bilal Abdul Muttalib Badawi. "Electronic Banking: What it is, its Transactions, and the Problems it Raises." In *Electronic Banking between Sharia and Law*, Dubai, 2003. p. 18.

and consumer protection. The EU's regulatory influence extends beyond its member states, shaping the legal and economic relations of neighboring states and trading partners through mechanisms such as association agreements, trade deals, and technical cooperation.[51] For example, Jordan has a Euro-Mediterranean agreement with the EU, which promotes alignment with EU standards in many areas.

Therefore, the use of EU legislation as a benchmark is of particular importance because it represents a sophisticated, codified, and comprehensive legal framework that has been adopted or adapted in many non-EU countries seeking to modernize their own regulatory systems. For Jordan, examining EU regulation provides a lens through which to assess how foreign legal systems influence domestic law, either through direct adoption or indirect harmonization. Moreover, such a comparison emphasizes the interplay between local needs and global influences, and highlights the opportunities and challenges Jordan faces in aligning with international standards. While Jordanian regulation remains distinct, the EU legal framework provides a robust and structured model for assessing regulatory development in a global context.

Moreover, Jordan's relationship with the EU, which was created through the Euro-Mediterranean Association Agreement and other cooperating frameworks,[52] highlights the importance of EU standards in the development of Jordanian regulation, several significant criteria drove the choice to utilize EU legislation as a comparative benchmark, for instance:

- The EU's role in setting global standards, the European Union is renowned as a global leader in establishing governance, commerce, environmental protection, human rights, and public administration norms. Many nations outside the EU adopt or adapt EU legislation, not only to promote commerce but also to update their legal systems in accordance with worldwide best practices. By researching EU law, this research gives insights into the ideas and procedures that support a globally important legal system, delivering useful lessons.

[51] Association Agreement - Jordan, Published by Ministry of Planning and International Cooperation of Jordan, Abstract;This document provides details of the trade-related commitments under the Jordan-EU Association Agreement, including aspects of regulatory cooperation that may impact on e-banking legislation, for more information see the link; available access on 18 December 2024, at; https://2u.pw/xpk5vs3P .

[52] Regulatory Alignment: The Euro-Mediterranean Agreement encourages economic and legal harmonization, making EU standards a natural starting point for Jordan's regulatory development.

- Jordan's Geopolitical and Economic Links with the EU Jordan has strong economic and political relations with the EU, as evidenced by trade agreements, financial aid programs, and technical cooperation efforts. For example, the Euro-Mediterranean Agreement promotes regulatory coherence in fields like as product standards, intellectual property rights, and competition policy. These agreements implicitly urge Jordan to align its regulatory framework with EU norms in order to improve worldwide compatibility and competitiveness.

- Regulatory Influence without Membership, EU legislation has a far-reaching influence, even on nations outside the Union, thanks to processes such as the "Brussels Effect," which sees EU policies copied internationally due to their strength and clarity. Jordan, like many non-EU nations, faces EU criteria while conducting cross-border commerce or negotiating alliances. Examining the impact of EU legislation provides a clearer understanding of how foreign legal systems influence local policies and practices, especially in the absence of official membership.

- Comparative Learning for Jordanian Regulatory Development, Jordan's regulatory structure has the combined problem of meeting local socioeconomic concerns while keeping flexible to global trends. Using the EU's highly codified and complex legal structure as a comparison model allows for a more nuanced evaluation of Jordan's regulatory strengths and opportunities for development. It also identifies areas where Jordan might strategically embrace or adapt EU approaches to strengthen its own governance structures.[53]

- Academic and practical relevance, from an academic standpoint, comparing Jordanian law to EU legislation provides an important case study of legal transplantation and adaptation in a non-member state. This research can provide practical suggestions for Jordanian policymakers, particularly in sectors where alignment with EU standards could improve regulatory efficiency, market access, or public welfare.

The following is a lengthy addendum that discusses the cooperative agreements and organizations, as well as the special context of e-banking and its regulatory obstacles between

[53] Policy Brief; How to Strengthen Jordan's Data Protection Law, Published by: Access Now, 2022, this policy brief conducts a comparative analysis of Jordan's draft data protection bill against the EU's General Data Protection Regulation (GDPR). It identifies areas where Jordan's legislation aligns with EU standards and highlights gaps that could be addressed to enhance data protection, for more information, available at: https://2u.pw/yvlzpKUY access on 17 December 2024.

Jordan and the EU. Jordan and the EU have a number of cooperation agreements and frameworks that govern their legal and regulatory relationship; this includes:

- The Euro-Mediterranean Association Agreement (2002); this agreement promotes strong economic and political collaboration between Jordan and the EU, with a focus on trade liberalization and regulatory alignment in areas such as banking, intellectual property rights, and industrial standards. The agreement sets a significant emphasis on harmonizing technical and legal frameworks to improve Jordan's access to European markets.[54]
- EU-Jordan Partnership Priorities (2016-2028); this strategy framework outlines consensus aims for economic transformation, including financial sector changes. A significant aim is to bring Jordan's banking legislation up to international standards, allowing the country to better integrate into the global financial system.
- The European Bank for Reconstruction and Development (EBRD); Jordan has received cash and technical assistance from the EBRD, with an emphasis on enhancing regulatory frameworks in banking, fintech, and digital financial services. The EBRD routinely collaborates with Jordan to implement best practices derived from EU laws.
- The EU-Jordan Compact (2016); this Compact focuses on economic resilience and reforms, such as digital transformation and financial inclusion measures. It indirectly pushes Jordan to adopt EU-compliant rules in the financial and digital sectors, particularly to fulfill the needs of financial aid and ongoing investment.

Indeed, the expansion of e-banking and digital financial services in Jordan creates prospects for growth while also imposing significant regulatory hurdles, particularly in terms of compliance with EU requirements. The revised EU Payment Services Directive (PSD2) creates a robust legal framework for electronic payments and financial services among member states, and focuses on security, consumer protection and innovation through open banking initiatives. Furthermore, the General Data Protection Regulation (GDPR) has established a global standard for data privacy and security, impacting e-financial services that rely heavily on consumer data.[55]

[54] The Euro-Mediterranean Agreement establishes an alliance between the European Community and the Hashemite Kingdom of Jordan Date of signature: 1997. Abstract: This Agreement serves as the foundation for ties between the European Union and Jordan, and it includes measures for economic cooperation and regulatory harmonization in a variety of areas, which may have an impact on electronic banking rules.

[55] The General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy regulation issued by the European Union (EU) that became effective on May 25, 2018. It is aimed to protect individuals'

Even though, when talking about the current regulatory framework in Jordan, Jordan has made progress in digital banking through the Electronic Transactions Law and the Central Bank of Jordan standards governing e-banking. However, gaps remain, particularly in data protection, cybersecurity, and interoperability of digital payment systems. While Jordanian regulations cover basic consumer protection, they are not as sophisticated as EU requirements such as PSD2, which requires third-party financial service providers to use secure and standardized interfaces. Jordanian banks are also facing growing concerns about cybersecurity. The Central Bank of Jordan has implemented cybersecurity guidelines, but they fall short of the rigorous protections required under EU rules.

In fact, Jordan's privacy regulations are not in line with the GDPR, posing issues for banks that work with EU-based companies or handle cross-border data transfers, among the most important of these points, Jordan's efforts to promote financial inclusion through mobile banking and fintech may conflict with strict compliance requirements based on EU standards, PSD2 has promoted open banking, but the idea is still in its early stages in Jordan. Challenges include the lack of legislative regulations for banks to provide standardized APIs, as well as limited regulatory assistance for fintech companies.

Undoubtedly, the digital banking cooperation between Jordan and the European Union, by highlighting these agreements, organizations and special cases in common, the thesis may clarify the multi-dimensional impact of EU standards on e-banking rules in Jordan while addressing the unique issues facing Jordan in this expanding field:

- Support for Fintech Development; Jordan has received financial and technical aid from initiatives such as the EU-funded SANAD Fund for MSMEs to improve its digital banking infrastructure, with an emphasis on underprivileged communities.
- Building Capacity for Digital Banking Regulation, the EU has offered technical training to Jordanian authorities, notably the Central Bank of Jordan, on how to build strong cybersecurity and anti-money laundering (AML) standards in digital banking.

personal data within the EU while regulating how corporations globally gather, handle, and store such data. The GDPR has become a global standard, affecting data protection regulations across the world, including Brazil's LGPD and California's CCPA. Its strong foundation stresses individual rights and corporate accountability, altering the way personal data is handled across sectors.

- Mobile Wallet Initiatives, Jordan has increased mobile wallet usage with the help of EU-affiliated organizations via platforms such as JoMoPay,[56] which allows unbanked people to make electronic payments[57]. While this constitutes an improvement, integration with EU banking systems remains an issue.

- Collaboration for E-payments, Jordanian banks have collaborated with EU firms to develop safe e-payment systems that meet international requirements. However, disparities in regulatory requirements, notably for PSD2 compliance,[58] indicate areas that require additional convergence.

In the same context, the relationship between the Jordanian banking system and the global financial system is of great importance, explaining how banking legislation and operations in Jordan adhere to or are affected by international standards and practices. A full discussion of the relationship between the Jordanian banking system and the global banking system is provided below. The Jordanian banking sector operates in a global financial context where compliance with international standards and participation in cross-border systems are of great importance for integration, competitiveness and stability; this is what was confirmed by one of the most important hypotheses on which this research was based; **eighth Sub-Hypothesis**, the extent to which EU regulations affect Jordanian regulatory frameworks, particularly in the context of challenges related to digital banking services, in terms of EU legislation being the most appropriate standard for Jordan, given its membership outside of the EU, and how the Jordanian banking system also meets the requirements of the global banking system. The following key elements underscore the links between the Jordanian financial system and the requirements of global banking:

- Adoption of international regulatory standards; Jordan has gradually linked its banking legislation with globally recognized norms to guarantee compliance and linkage to the

[56] EU and World Bank Influence: The use of mobile payment systems such as JoMoPay demonstrates Jordan's adherence to international financial frameworks and commitment to digital financial inclusion, which is consistent with World Bank and IMF recommendations.

[57] JoMoPay is an electronic system that provides instant mobile payment services, where mobile wallets are registered on the system for the purpose of exchanging financial transactions between mobile wallets and to and from bank accounts. The JoMoPay system was officially launched in 2014 as a result of radical changes that occurred in mobile payment services in terms of storing small financial values and transferring them to others to meet their financial needs, for more information, available at https://2u.pw/gCg0De1X , access on 14 December 2024.

[58] The Revised Payment Services law (PSD2) is a European Union (EU) law that regulates payment services and payment service providers within the EU and the European Economic Area (EEA). Its key goals are to increase consumer protection, innovation, and payment security.

international financial system. The Central Bank of Jordan (CBJ) follows the Basel III framework,[59] which prioritizes capital adequacy, liquidity management, and risk assessment. This alignment guarantees that Jordanian banks fulfill the resilience and transparency standards set by internationally networked institutions, in the same context, Jordan is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF), which supports worldwide standards for anti-money laundering and counter-terrorism financing. These methods promote international trust and connection.

- Participate in international financial institutions; Jordanian banks are linked to global banking networks by their participation in international financial institutions; Jordanian banks utilize the SWIFT network for safe cross-border financial transactions that align with international payment systems, Jordanian banks have correspondent links with global banks, enabling them to conduct international transactions and access overseas markets. Jordan's compliance with World Bank and IMF recommendations demonstrates its commitment to aligning its banking sector with global financial frameworks. [60]

- Use of global payment systems; the Jordanian banking system promotes cross-border transactions by participating in international payment networks. Credit card processing systems, including Visa and Mastercard, are fully functioning in Jordanian banks use regional and worldwide clearing networks to facilitate international trade finance and remittances. [61]

- Comply with global data protection and cybersecurity standards, to stay internationally linked, Jordanian banks must conform to data protection and cybersecurity regulations, many Jordanian banks use ISO 27001, an international standard for information security management, efforts

[59] The Basel III framework is a set of international banking laws designed by the Basel Committee on Banking Supervision (BCBS) to improve bank regulation, supervision, and risk management internationally. It was implemented in response to the 2008 financial crisis to increase the banking sector's ability to absorb shocks and lower the danger of systemic failure.

[60] Jordan—Financial Sector Assessment Program and Financial System Stability Assessment, Published by the international Monetary Fund, 2023, Summary: This assessment evaluates Jordan's financial sector stability and highlights the country's compliance with international financial standards and recommendations, for more information, available at https://2u.pw/YekDgXMY access on 16 December 2024.

[61] Mastercard Partners with Central Bank of Jordan to Build a More Robust Digital Payment Ecosystem in the Kingdom, Published by: Mastercard Newsroom, 2024, this press release details the collaboration between Mastercard and the Central Bank of Jordan to enhance the digital payment ecosystem, reflecting ongoing efforts to align with international standards, for more information, available at https://2u.pw/vKWNHH0w access on 16 December 2024.

are underway to conform with GDPR-like data protection laws to ensure secure cross-border data transfers, especially with European nations.

- Integration of FinTech and Digital Banking Innovations, Jordanian banks have adopted innovative solutions that correspond with worldwide fintech principles, driven by the global trend toward digital transformation in banking. JOMO PAY, established by Jordan's Central Bank, aims to deliver interoperable payment options. Collaboration with multinational fintech businesses has led to the introduction of blockchain-based technology and digital wallets, enhancing global financial connection.

- Difficulties in Connectivity with Global Banking, regardless of these efforts, Jordan's financial sector has many hurdles in fully integrating with global banking systems; regulatory gaps in data privacy, cybersecurity, and digital banking hinder integration with global best practices, regional instability can impair Jordan's financial connection with specific jurisdictions, cost of compliance, meeting international regulatory criteria, such as Basel III, imposes financial and operational burdens for Jordan's smaller banks.

- Cooperation with international partners: The Jordanian banking system receives technical assistance from foreign organizations, such as the European Bank for Reconstruction and Development, which encourages regulatory changes and digital banking innovation. For example, the Arab Bank, which is headquartered in Amman but has a global presence, works to connect Jordanian banks to foreign markets.

Thus, Jordan's banking sector's link to the global and EU banking system demonstrates the country's commitment to adopting international financial principles. Jordan's banks have positioned themselves as active participants in the global financial ecosystem by adopting global standards, joining international financial organizations, and incorporating fintech technologies. Addressing current gaps in legislative frameworks and technical infrastructure would strengthen Jordan's global connection and competitiveness; this is what was confirmed by one of the most important hypotheses on which this research was based; **eighth Sub-Hypothesis**, the extent to which EU regulations affect Jordanian regulatory frameworks, particularly in the context of challenges related to digital banking services, in terms of EU legislation being the most appropriate standard for Jordan, given its membership outside of the EU, and how the Jordanian banking system also meets the requirements of the global banking system.

In the same context, i will explain an important example of the most important aspects of the connection and relationship between the Jordanian banking system and one of the most important requirements of the current global banking system; Jordan has integrated SWIFT primarily for international transactions, especially within its trade partnerships in Europe. For example, "Jordan's use of SWIFT is most evident in its transactions with important partners in Europe and the Gulf Cooperation Council.[62] Currently, Jordan's use of SWIFT is strong for trade-related payments, particularly with its partners in the European Union. To build on this; for example, the Central Bank of Jordan has enabled seamless international transactions through SWIFT for remittances, which represent a significant portion of the country's GDP. Remittances accounted for nearly 8% of Jordan's GDP in 2022, with the majority of these transactions being processed through SWIFT. Furthermore, Jordan's reliance on correspondent banks such as Citi and Deutsche Bank demonstrates its connectivity to global financial networks.

However, challenges such as high transaction costs and compliance requirements with growing international rules, such as those set by the Financial Action Task Force, still provide opportunities for development. This highlights a solid foundation, but there are still opportunities to expand its network into emerging markets. As result, Jordan's use of the SWIFT network demonstrates its commitment to integration with the global financial system. This integration not only promotes international trade and remittances, but it also improves the general efficiency and security of the country's financial operations.

In addition to the above, blockchain technology is being considered for transparency in transactions. Additionally, diversifying banking relationships Correspondence to include strategic alliances in Asia can mitigate the risks associated with over-reliance on certain regions.[63]

the dissertation stresses the significance of this dynamic while keeping the larger concerns of Jordanian regulation separate. This method not only reveals the EU's effect on Jordanian law,

[62] SWIFT; stands for the Society for Worldwide Interbank Financial Telecommunication. It is a globally recognized messaging network that enables secure and standardized communication between banks and financial institutions for international transaction.

[63] initiatives like CIPS (China's Cross-Border Interbank Payment System) or ASEAN Payment Connectivity can offer alternatives to existing systems like SWIFT.

but it also helps to get a better understanding of how global legal norms interact with national systems in a complicated geopolitical setting.

As a researcher, I believe that the European model is a model that deserves to be compared to it, as it is an advanced model, and many countries are seeking to search for advanced regulatory models in this sector, as it is a sensitive sector and requires the solidarity and integration of all expertise in this regard, as the EU is a large union of countries, and it has multiple experiences and feedback from all countries about the appropriate methods of protection from the fraud operations they face, and there is no doubt that the legislators in the EU are working to develop these regulations through the different opinions and feedback provided to them by the members present in the EU, so I decided to move to this union, which adds value in the sphere of legal regulation of electronic banks.

I. 4. Legal Framework For The Liability Of The Electronic Authentication Service Provider In Jordan & EU

The challenges confronting electronic banks and impeding their proliferation necessitate advanced protective measures, among which electronic certification certificates stand out as crucial tools. It is imperative to delve into this topic as it offers substantial benefits in safeguarding the electronic financial system within electronic banks**.** Understanding the legal regulatory tools used to mitigate risks in electronic banking is essential to assess the extent to which the Jordanian Electronic Transactions Law complies with international standards. This is in fact the basis of **the research question**, which focuses and revolves around the essence of exploring the preventive legal mechanisms provided by electronic authentication certificates, especially with regard to the encryption of communications between client browsers and servers (SSL/TLS). As is known, these certificates play a pivotal role in protecting data from eavesdropping and tampering during transmission, which is very important and is at the heart of one of the most important research hypotheses "regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system"**.** Furthermore, electronic certification certificates ensure that clients connect to the legitimate server, thwarting

potential phishing attacks. This aspect underscores one of the critical **hypotheses** that necessitates examination the extent to which regulators must devise comprehensive crisis management strategies to address potential operational failures or electronic intrusions that could disrupt the electronic financial system. Additionally, compliance with Know Your Customer (KYC) requirements, particularly in relation to anti-money laundering (AML) measures, warrants careful consideration in the regulatory framework.

To achieve this, the Jordanian legislature must undertake a comparative analysis of legislation governing the responsibilities of authentication service providers for electronic signatures between the European Union and Jordan. This comparison aims to ascertain the level of harmonization in regulatory frameworks concerning the operations of electronic signature service providers. Emphasis is placed on evaluating the sufficiency of overarching regulations in overseeing the obligations of electronic service providers under Jordanian law. It underscores the critical importance of developing dedicated regulations tailored to the specific responsibilities in this domain. Specialized rules are deemed necessary, particularly concerning alignment with international legislation on electronic signatures and directives outlined by the European Union. This confirms the importance and truth of the **research question posed**; "To what extent does the Jordanian Electronic Transactions Law conform to the rapid legislative developments of electronic banks in light of the transformation of international standards and the European Union**"** this approach ensures compliance with global standards and enhances the effectiveness of regulatory oversight in the realm of electronic signatures[64].In recent times, there has been a notable surge in the interest of countries to draft and enact legislation aimed at establishing the necessary legal framework for electronic commerce while removing barriers to its growth. This heightened focus seeks to instill confidence in online transactions by ensuring secure methods for verifying customer identities and safeguarding information transfers. In a virtual landscape fraught with considerations regarding the security and integrity of electronic transactions, there arose a compelling need to instill the utmost confidence in these transactions. This necessitated the verification of the validity of contracts and their attribution to the appropriate entities. Hence, electronic writing and signatures have emerged as instrumental tools

[64] Ali, Jaber. *Factors Affecting Electronic banking Adoption in India Evidence from the World Bank's Global Financial Inclusion Index Survey*. Journal of Developing Regions. Vol. 57, Issue 2, Spring 2023. p. 341.

aligning with the nature of electronic transactions. Among these tools, electronic signatures have emerged as a pivotal component of electronic commerce, with various forms such as pen-based electronic signatures and biometric signatures gaining prominence[65].Resorting to electronic signatures presents challenges surpassing those of traditional handwriting, particularly concerning confidence in attributing signatures to their owners. This uncertainty can hinder trust in electronic transactions, as verifying the authenticity of electronic signatures and linking them to their owners may pose difficulties for counterparties. Therefore, there is a pressing need for a neutral and trusted intermediary to facilitate authentication between senders and recipients. Consequently, the importance of digital signatures and the establishment of a reliable system to verify their validity become paramount[66]. In order to verify the authenticity of digital signatures and establish a direct connection with their owners, electronic authentication utilizes a system where an electronic authentication service provider issues an electronic certificate. This certificate includes precise components and information required by legislation to confirm the authenticity of the digital signature and guarantee its proper attribution to its proprietor. During this procedure, the certifying authority confirms the integrity and authenticity of the information stored in the certificate. This instills confidence in the integrity of the transaction being submitted, reassuring others of its authenticity.

The task has been undertaken by electronic authentication service providers who serve as intermediaries between the parties involved. These providers are governed by a specific legal framework, which is regulated by specialized rules in the electronic transaction laws of various countries. However, the Jordanian Electronic Transactions Law does not provide clear, precise, and detailed guidelines on how to issue electronic certificates, as it comes in an attempt to highlight the extent of harmony and harmonization in the Jordanian Electronic Transactions

[65] The purpose of this text is to examine the idea and consequences of digital signatures and certificates of authenticity, see Assistant A., *Digital Signature and Certificate of Authenticity: Concept and Legal Implications*, "Al-Manara Journal - Al al-Bayt University". Vol. 11, No. 4. p. 249, 2005, and also see online for more information on. p. 66-58, 2004, London, Well Max and Sweet *» Regulations and Law: Electronic Signatures* , Brazil L., Rice B., *Development of Electronic Evidence and Evidence* , "American Bar Association Publication". 2008. p.11.

[66] Hassan L., *Electronic Documentation and the Responsibility of the Competent Authorities*, Dar Al-Raya for Publishing and Distribution, Amman, 2009, p. 101. and beauty S., *Contracting through Modern Communication Technologies*, Dar Al-Nahda Al-Arabiya, Cairo, 2006, p. 321. & Al-Sabahin S., *Electronic signature and its authenticity in proof*, unpublished doctoral thesis, Amman Arab University for Graduate Studies, Jordan, 2005. p. 156.& BRUN M., *Nature et effects juridiques de la certification dans le commerce électronique sur Internet, March* 2000, more information, see https://www.lex-electronica.org/files/sites/103/7-1_brun.pdf (accessed January 25, 2023).

Law, and using the texts of comparative legislation that have previously regulated the subject. Accurately, the complexity involved in proving the traditional conditions of responsibility prompted legislators in many countries to regulate them with special provisions, and this topic is considered one of the recent studies that have not been addressed in Jordan, and the need comes here to alert the Jordanian legislator to the need to intervene to regulate the electronic documentation process and the responsibility that it entails, and given the role that this process plays in facilitating and flourishing[67] e-commerce. For example, the French legislature was in line with the European Union directive and regulated this process with the Trust Act,[68] which established a special liability for providers of electronic authentication services in the formal economy, inspired by the provisions of the European Union Directive.

In this regard, the topic of electronic authentication services presents several legal challenges that can be addressed by specific legislation. The legal character, legal foundation, and establishment of responsibility for electronic authentication service providers are still under discussion in legal doctrine. Furthermore, the Jordanian legislator has not established a specific legal framework to address the liability of the electronic authentication provider, leaving several uncertainties regarding the scope of liability and the determination of compensation for damages to customers or third parties.[69]

The absence of a dedicated legal framework for third-party liability in Jordan prompts questions about compensation and accountability for damages incurred by customers or third parties in relation to electronic authentication services. This section aims to address these uncertainties by examining whether existing general liability provisions adequately encompass issues pertaining to electronic documentation providers. It also seeks to assess whether there's a need for the Jordanian legislature to establish specific regulations governing the accountability of electronic authentication service providers. Through a broad-ranging exploration, this section aims to offer

[67] E. Caprioli, "La directive européenne n 1999/93/13 décembre 1999 sur un cadre communautaire pour les signature électronique," *Gazette du palais*, October 2000, accessed January, 2023. p. 7. https://www.caprioli.ts.com/migration/pdf/signature_confiance_signelec.pdf

[68] Le Tourneau P, *Contrats du numérique 2022/23 12ed - Informatics and Reliable Electronics* – The Great Form of the Book, 2022. p.39.

[69] Khams, captivating A. *The Impact of Digital Transformation on Employment Strategy in the Banking Sector: A Case Study of Egypt.* Revista de Management Comparat International. July 2022, Volume 23 Issue 3. p. 457.

comprehensive insights into the legal landscape concerning electronic authentication services in Jordan.[70]

As is known, the Jordanian Electronic Transactions Law was noticeably limited to provisions dealing with the civil liability of authentication service providers, and imposed financial penalties and fines for providing false information, which necessitated resorting to general rules to determine the legal liability of electronic authentication service providers, which confirms the main **hypothesis** of the research. Legislation has been implemented to limit identity theft and fraud in online banking. However, authorities are encountering challenges in establishing secure and authenticated digital identity procedures. New laws have been introduced to protect electronic bank customers, ensuring transparency in fees, conditions, and dispute resolution systems. Although the ITU Financial Services Act contains certain general rules on outsourcing, the monitoring of the contractual dimension is not well established and communications from third parties, the external source of ICT risks is not comprehensively addressed.

Thus, it is necessary to completely incorporate certain provisions into the legislation of the Union. Given the lack of explicit and comprehensive ITU standards regarding contractual agreements with IT service providers, financial entities rely on the Basic Principles for Guiding the Management of Third-Party ICT Risks. These principles are especially crucial when financial entities seek assistance from ICT third-party service providers for their critical or important operations. These principles should be accompanied by a set of fundamental contractual rights concerning various aspects of contractual agreements, in order to establish minimum safeguards that will enable financial entities to effectively monitor all ICT risks that arise on a global scale.

The standards regarding third-party service providers complement the sector-specific laws governing outsourcing practices.[71]

European Union legislation appears to be influenced by the European Union Directive on Electronic Signatures that has adopted the liability regime for electronic authentication service

[70] S.D., Kavitha Vanni. Electronic banking Units: Perception and Acceptance of Customers in Rural India, Journal of Bank Management. November 2022, Volume 21 Issue 4. p. 10.
[71] Act (I/29), Regulation (EU) 2022/2554 of the European parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

providers.[72] This compels us to investigate the key components of this system in order to urge the Jordanian legislature to contemplate this law and use its methodology in formulating specific regulations to govern the legal obligations of authentication service providers in Jordan. The potential responsibility arises from the service provider's failure to comply with the legal responsibilities set forth in the legislation governing the electronic authentication procedure. Thus, we examine the legal liability of electronic document service providers. It is worth noting that the unique nature of the electronic authentication process and the intricate relationships that arise from issuing electronic certificates warrant the consideration of various liability scenarios related to electronic authentication services. This allows for the possibility of both contractual liability on the part of the responsible party of the provider towards the certificate holder, as well as default liability on the part of the service provider towards others.[73]

The electronic authentication contract governs the interaction between the provider of electronic authentication services and the certificate holder. Furthermore, there exists a connection between the service provider and external entities that depend on the electronic authentication certificate to finalize specific operations.[74] The certificate holder has a connection with others that revolves around a contract they want to establish, which pertains to the provision of particular products or services.[75] This raises the issue of liability for damages caused by a defect in the electronic authentication process. It is important to determine whether the service provider or the customer holding the certificate can be held liable for such damages. Additionally, it is worth considering whether it is possible to exempt or restrict the service provider's liability.

I. 3.1. Service Provider Contractual Framework

Contractual liability arises from the occurrence of damage resulting from the debtor's breach of an obligation resulting from the beneficial contract, and this breach is either the debtor's

[72] Directive 93/13/EEC protects consumers in the EU from unfair conditions and is amended by Directive (EU) 2019/2161.
[73] Sarhan A., Khater N., *Sources of Personal Rights*. Dar Al Thaqafa for Publishing and Distribution", 2021. p. 302.
[74] Mell, p&d dray j., & shook, j, *Unified identity management for smart contract without third-party authentication services*, Bonn. 2019. p. 15.
[75] Lim, SY, Fotsing, PT, Almasri, A, Musa, O, Kiah, MLM, Ang, TF & Ismail, R, *'Blockchain Technology the Identity Management and Disable Authentication Service: Survey"*, "International Journal of Advanced Sciences, Engineering and Information Technology". Malaysia, 2018, Vol. 8, No. 4-2. pp. 1735-1745.

failure to perform his obligations or an existing and blatant contract, and therefore the customer with the certificate of authenticity may suffer from a defect in implementation or even a delay in whole or in part in implementation, and the application of damages as a result of the notary services provider's breach of one of its obligations under the notarization contract concluded between them or under the text of the law.[76] The notarization provider and the client holding the certificate have the authority to establish mutually agreed-upon terms and obligations in the event of a breach by the service provider. This is in line with the principle of contractual freedom and authority. If either the notary services provider or the customer assumes such obligations, they will be contractually liable for any inaccuracies in the issuance of this certificate [77]. At the same time, contractual liability arises, as the electronic authentication contract imposes mutual obligations on both parties, and any breach by the service provider or the certificate holder of the obligations incumbent on each of them evaluates their contractual liability. It is often stated in this contract that the service provider is obliged to confirm and verify the authenticity of the data contained in the certificate with the contracting parties, if attributable to the holder of the electronic signature, even if it is not specified by a special provision in the law, because this obligation constitutes the essence and basis of the electronic authentication process.[78]

Based on the above, the parties are allowed to include elements in the electronic authentication contract that define the provider's responsibility to protect the personal data of the customer who got the certificate. These provisions may restrict the utilization, manipulation, or dissemination of such data to external entities without the customer's explicit agreement. Furthermore, the service provider may be obligated, in such circumstances, to abstain from modifying or deleting any customer-related data without the explicit approval of the individual. Consequently, the Service Provider is legally obligated to take responsibility for any violation of the duty to generate, utilize, or exchange such data without the Customer's consent. The suspension or cancellation of the electronic certification certificate is governed by the Jordanian Electronic Transactions Law, which imposes penalties for non-compliance. However, if the customer and service provider agree on the obligation to suspend or cancel the certificate, or if there are valid

[76] For more information on the nature of the contractual relationship between the certification services provider and the signatory, see Plotkin, M., *E-Commerce Law and Business*, "Aspen Publisher". United States of America, 2003.
[77] Trudell P., Abran F., Penikalf K., Heine S., *Cyberspace Law, Montreal*, Themes Editions, 1997. p. 3.
[78] Mel B., Dray J., Shock J., *Unified identity management for smart contract without third-party authentication services, Bonn*, 2019. p. 7.

reasons for doing so, the service provider's contractual liability must be based on any damages resulting from their failure to fulfill this obligation.[79]

This principle can extend to any breach of obligations outlined in the electronic documentation contract. In such cases, the provider's contractual liability arises from the breach, and the supplier's responsibility towards third parties can be envisioned if there exists a direct contractual relationship. If the breach of contract results in damages, these damages may be assessed considering the electronic documentation of the third-party service provider. For instance, if a third party relies on a certificate issued by the service provider as per a contract, and it later turns out that the certificate is invalid, revoked, or suspended without notifying the certification services provider, damages may ensue. This is because the third party entered into contracts with the customer based on the trust established from the electronic certificate, which was compromised[80]. In this scenario, establishing a jurisprudential relationship between the provider and the third party involves examining how the certificate was obtained. Was it obtained directly through the provider [81], or was there another intermediary involved, such as the certificate holder or another authentication provider? Third parties might acquire certificate of authentication and a public key through various means[82]. Understanding the specific process through which the certificate was obtained is crucial in determining the nature of the relationship between the provider and the third party in legal terms.

If the third party obtains the certificate of authentication and the public key directly from the holder of the certificate, herein facing a contractual relationship between the provider and the foreigners of third parties, and therefore it is not possible to imagine the contractual responsibility of the provider, but it is a damage that third parties may obtain the certificate of authentication and the public key from the provider as a result of a contract[83], which leads to the possibility of conceiving a contractual relationship between them, linked by the third party to

[79] Article 25 of the Jordanian Transactions Law of 2015, previous reference.
[80] Qasim A., *Some Legal Aspects of Electronic Signature*, Law and Economics. 2002, No. 72. p. 32.
[81] To get knowledge about the notion of public key in electronic authentication and its technical functioning, see "Masaa A", *Digital Signature and Certificate of Authenticity: Concept and Legal Implications*", "Al-Manara Magazine-Al al-Bayt University". 2005, Vol. 11, No. 4. p. 249. See also UNCITRAL, Enhancing Confidence in Electronic Commerce: Legal Issues Concerning the International Use of Electronic Authentication and Signature Methods, United Nations publication, 2009.
[82] Yaqoub A., *Civil Liability of a Digital Signature Certification Services Provider to Third Parties*, Bahrain Law Journal. Vol. III, No. I, 2006. p. 304.
[83] Jacob A., *Civil Liability of the Certification Service Provider*, op. cit., p. 313.

the notary services provider and thus the possibility of lifting the rules of contractual liability if the third party who relies on these Certificate no damages.[84]

Contractual liability for damages suffered by third parties can be contemplated when these third parties rely on the certificate issued by the service provider. Such reliance can lead to damages for third parties who trusted the electronic authentication certificate and its accreditation. Therefore, the service provider may bear contractual responsibility for these damages incurred by third parties due to their reliance on the certificate[85]. Indeed, the contractual duty of the electronic authentication service provider generates various nuanced problems that the general standards may insufficiently address, aggravating the implementation challenges. Proving the error of the electronic authentication provider is often exceedingly arduous, compounded by the absence of a discernible contractual relationship between them and the contract owner, rendering it practically inconceivable in many instances. The proliferation of relationships stemming from this lack of clarity, coupled with the intricate and contemporary nature of diverse electronic signature techniques and authentication certificates, further complicates matters. Determining the nature of the service provider's obligation poses a profound quandary: is it an obligation of meticulous care or the attainment of a specific result? This ambiguity significantly amplifies the burden of proof, rendering it notably formidable to substantiate claims in such cases[86]. Undoubtedly, parties can circumvent these challenges through the terms outlined in the electronic authentication contract. Consequently, it is essential for parties to exercise vigilance and caution when drafting the contract terms, especially those concerning exemption and mitigation of liability. Many such conditions could be perceived as arbitrary or infringing. Notably, the EU Directive on unfair terms, dated 5 April 1993, applies to the relationship between customers and suppliers, ensuring consumer protection against unfair contractual terms.[87] Directive 93/13/EEC safeguards European Union customers from unjust terms and conditions that could be present in normal contracts for the products and services they acquire.

---

[84] Public key: The code assigned or approved by the user's electronic certification authorities as an electronic authentication certificate to verify the authenticity of the electronic signature. According to Article 2, Electronic Transactions Law No. 15 of 2015.

[85] Abul-Lail I., *Documentation of electronic transactions, burning, nature and legal impact,* 2018. & BRUN M., *Nature et effects juridiques de la Certification dans le Commerce électronique* sur Internet, Mars 2000, more information see, https://www.lex-electronica.org/files/sites/103/7-1_brun.pdf access on Feb 2023.

[86] Sarhan A., Khater N., *Sources of Personal Rights*, Dar Al-Thaqafa for Publishing and Distribution, 2021. p. 302.

[87] "Directive 93/13/EEC was amended by Directive (EU) 2019/2161, which aims to update EU consumer law and improve its enforcement".

The new contract for consumers incorporates the notion of "good faith" in order to avoid any substantial disparity in the reciprocal rights and responsibilities of the parties involved.

In the same context, the Jordanian Electronic Transactions Law does not include provisions specifying conditions for the responsibility and legal framework of submitted documents. In the absence of such specific provisions, the liability of the electronic notary service provider is determined by Jordanian legislation. This necessitates referring to general rules on civil liability, whether contractual or tortious. Various states have shown interest in enacting legislation to ensure trust and confidence in such transactions.

To mitigate the systemic implications of third-party ICT concentration risks, the Regulation encourages a step-by-step and adaptable approach. Financial institutions must evaluate their contractual agreements to determine the likelihood of such risks, especially when entering into agreements with third-party ICT service providers in a foreign country. "Strict restrictions and limits on third-party exposure to ICT are not suitable for achieving a reasonable balance between contractual freedom and financial stability. The lead controller appointed in accordance with the Regulation shall be aware of the interdependence of third-party ICT service providers and detect cases where excessive concentration may compromise the stability and integrity of the financial system of the Union. To fully monitor the risks that may arise from third-party ICT service providers, which depend heavily on the stability, functionality, availability, and security of ICT services received, it is necessary to align the main contractual elements with these service providers".[88]

In an extensive look at the legal rules and principles regarding service provider ratifications and the most important regulatory benchmarks in this regard, the use of electronic signature methods in international contracts benefits from the adoption of common standards for electronic and paper digital signatures.[89] "Functional equivalence standards between electronic and paper signatures could provide a common international framework to allow electronic authentication

[88] Act (I/69) " When renegotiating contractual arrangements to seek alignment with the requirements of this Regulation, financial entities and ICT third-party service providers should ensure the coverage of the key contractual provisions as provided for in", Regulation (EU) 2022/2554 of the European Parliament and of the Council Of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[89] Trudell P., Abran V., Benikhlev K., Hein S., *Cyber Law*, faculty of law of the university of montreal, centre for research in public law. themis editions, 1997.

and signature methods to meet signature requirements".[90] However, There appear to be ongoing issues about the global implementation of these approaches, which necessitate the participation of a reliable third party in the authentication or signing procedure.[91] and for this purpose the reciprocity and verification of the place of origin must be searched.

I. 3.2. Place Of Origin Reciprocity And Local Verification

A crucial responsibility of a local certification services provider, certification authority, or regulatory authority is to acquire country-specific signatures and certificates for the purpose of verification. These signatures and certificates are legally issued between countries based on reciprocity. Recognition systems may unintentionally exhibit discriminatory effects. For instance, in a non-EU country, there are three choices for certificate recognition. Certification service providers must adhere to the requirements of the EU Directive on Electronic Signatures and obtain accreditation from a system established in an EU Member State.[92] " The Directive effectively requires foreign certification service providers to comply with both the regulations of their country of origin and those of the European Union which is a higher standard than what is required of certified certification service providers in a member state. In addition, the EU Directive on Electronic Signatures has been implemented with some deviations. Ireland and Malta, for example, recognize foreign digital signatures (certifiable certificates in EU terminology) as equivalent to domestic signatures provided other legal requirements are met. On the one hand Other, recognition is subject to domestic verification (Austria, Luxembourg) or to a decision by a local authority (Czech Republic, Estonia, Poland) This tendency to insist on a form of domestic verification, usually justified by legitimate concerns, regarding the reliability of foreign certificates, leads in practice to a system of differentiating foreign certificates according to their geographical origin. The EU Directive on Electronic Signatures

[90] Berhan Moges Adonya, Krishna Gadasandula, and Swapna Dharavath, "Effects Of Technology-Based Innovation On The Financial Performance Of Listed Commercial Banks In Ethiopia: The Case Of Electronic Banking," *Turkish Online Journal of Qualitative Investigation* 12, no. 8 (2021), pp. 66-87.

[91] UNCITRAL Commercial Law Enhancing Confidence in Electronic Commerce: Legal Issues Relating to the International Use of Electronic Authentication and Signature Methods, United Nations, Vienna, 2009.

[92] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repeal of Directive 1999/93/EC Article 25/3 Legal effects of electronic signatures: An eligible electronic signature based on an eligible certificate issued in one Member State must be recognized as an eligible electronic signature in all other Member States.

requires foreign certification service providers to comply with both their original data and the EU regime which is a higher standard than Certification services accredited in a member state of the European Union". [93]

Article 6 of this directive included a legal regime for the liability of the specialized electronic authentication services provider, to confirm this trend, that authentication services have specific rules according to the nature of the tasks performed by these providers and the role they play due to the strong dominance of the electronic authentication process in the Internet Contracting and commercial trust, and the directive was accompanied by several rules highlighting the specificity of the rules of responsibility for services that distinguish electronic documents from the general rules of responsibility. In the same vein, the EU Directive established the legal regime for supplier liability on several grounds, inter alia, the obligation to distinguish between an accredited electronic certificate and a non-certified certificate. It has also resorted to stricter supplier liability, as it is assumed (the EU directive has also made it possible to limit the extent or scope of its liability, unless the service provider proves otherwise).[94]

In a case law with a common context in this context," on 11th November 2020, the Court of Justice of the European Union held that the Near Field Communication (NFC) function of a bank card, also known as contactless payment, is itself a "payment instrument" as defined in the EU Payment Services Directive 2015/2366 PSD 2, and the CJEU also clarified the meaning of "anonymous use" under PSD 2 about the NFC function. The court stated that the bank may not exclude its liability for low-value transactions that are not authorized in its general terms and conditions by simply claiming that blocking the NFC function would be technically impossible but must prove impossible in light of the objective state of the technical knowledge available when the customer reports a lost or stolen bank card. Furthermore, the Court ruled that if the user is a consumer The General Terms and Conditions provide for tacit consent to future amendments to these Terms and Conditions and must comply with the review standard set out in Directive 93/13 on the Protection of Consumer Rights, and not with PSD2, it defines the responsibilities required of each party and defines the responsibility of the certification service

[93] Article 7, EU Directive on Electronic Signatures, Article 7, Eligibility for notification of electronic identification schemes an electronic identification scheme shall be eligible for notification pursuant to Article 9(1).
[94] Sedallian. "*Development of Electronic Commerce, New Trade of the Convention*, accesses on Feb 2023" *www.droit-technologies.com*, 2000. p. 5.

provider, which determines the actions of the authorized party. The relying party shall bear the legal consequences of failure to do so; (i) take reasonable steps to verify the authenticity of the electronic signature, (ii) if the electronic signature is supported by a certificate, reasonable steps shall be taken".[95]

The idea seemed to be that a party intending to rely on an electronic signature should consider whether such reliance was reasonable in the light of the circumstances and to what extent.[96] This statement does not discuss the validity of the electronic signature, as that is covered in article 6. The validity of the electronic signature should not be influenced by the actions of the relying party. It is important to separate the question of the signature's validity from whether it is reasonable for the relying party to trust a signature that does not meet the standard outlined in article 6.[97]

Consumer concerns Although Article 11 may impose difficulties on authorized parties, particularly when they are consumers, it is important to remember that the Model Law does not aim to invalidate any consumer protection regulations. However, the Model Law can still serve as a valuable tool in educating all relevant parties, including authorized individuals, about the appropriate standard of behavior when it comes to electronic signatures. Furthermore, it may be deemed vital for progress to define a set of rules that require the relying party to verify the legitimacy of the signature using easily available methods.[98]

The Model Law on Electronic Signatures in 2011 clearly delineates the duties and legal obligations of all parties involved, particularly specifying the responsibilities of the certificate authentication service provider. This legislation establishes specific protocols for the party receiving the license and imposes legal responsibility on the party relying on an electronic signature if they do not make reasonable efforts to confirm its validity. When an electronic signature is accompanied by a certificate, the party relying on it must undertake reasonable measures to verify that the certificate has not been revoked or invalidated, and to comply with

[95] The case before Court, European Court of Justice *Governing the liability of banks for unauthorized low-value transactions using contactless payment* "Library of Congress" https://cutt.us/hqnwX Accessed January 02, 2023.
[96] Gyurazar, Nada. Comforter, Hamid; Comforter, Hadi, *Investigate the impact of COVID-19 restrictions on the adoption of electronic banking technology among middle-aged customers in the Iranian banking industry.*, Turkish Magazine Online For qualitative investigation، Volume 12 Issue 8،2021. p.57.
[97] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, United Nations, New York, 2001.
[98] Article 11 of the UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, United Nations, New York, 2001.

any limitations associated with the certificate. According to Article (11), the party who plans to use an electronic signature must evaluate whether it is acceptable to rely on it based on the specific situation. This clause aims to guarantee the cautiousness of the relying party, without considering the legitimacy of the electronic signature, which is discussed in Article 6 and should not be influenced by the actions of the relying party.

In addition, "the establishment of a standard of conduct whereby the relying party must verify the authenticity of the signature by accessible means may be considered essential for the development of any public openness infrastructure system".[99]

Dependence on the rationality of utilizing the certificate of authenticity as a requirement for the legal responsibility of the service provider is crucial in striking a balance between safeguarding others and preventing excessive duties on the service provider. If a third party cannot reasonably trust a faulty authentication certificate because of previous contacts with the certificate holder or the kind of transaction, it would be unfair to hold the notary service provider responsible. If there are valid reasons based on general liability principles, such as force majeure, activities of third parties, or actions of the injured party, the service provider may not be held responsible for any losses caused by the electronic document.

When it comes to establishing force majeure as a justification for the supplier's refusal to accept responsibility, the supplier's duty for the harm incurred may be nullified if it can demonstrate that the damage was caused by an uncontrolled factor and was the consequence of an unforeseeable incident that was beyond its control. The cause must be extraordinary and outside the control of the parties, such as the inability of a foreign corporation to fulfill its obligations.[100] It is required to be unforeseen, including events like earthquakes, volcanic eruptions, wars, or floods, that result in damage to electronic devices used in electronic authentication processes. I agree with this perspective.[101]

It is noted that "these cases involve the non-liability of the service provider due to the actions of the customer holding the certificate or decisions based on general liability rules. Thus, the

[99] Article 11 of the UNCITRAL Model Law, op. cit.
[100] Abdul Hussain Jassim Muhammad, Manaf Abdul Kazim Muhammad, and Ahmed Hussein Ahmed, "*The Impact of Banking Risk on Electronic Banking: A Comparison* " *TEM Magazine* 10, no. 2 (May 2021), pp. 663-670.
[101] Ibid, pp. 663-672.

provider acted as a third party, not due to force majeure, which pertains to damage caused to others despite suspending or canceling the certificate at an irresponsible request".[102]

Similarly, if the certificate holder does not uphold the confidentiality of their electronic signature password or fails to notify the service provider if a third party gains access to or takes control of the private key, or if any alterations to the data occur after the certificate is issued, the service provider's responsibility may be invalidated. Moreover, if it can be proven that it is illogical for a third party to trust an electronic authentication certificate, for example, when the certificate has been suspended or permanently revoked, and this information is documented in the electronic certificate register that the service provider is required to maintain, then this would serve as a legitimate justification for why the service provider cannot be held responsible for any harm caused by the unreasonable trust placed on the electronic certificate.

Herein, there is no denying the lack of compatibility and harmony between Jordanian laws and the above-mentioned European legislation. Through this, the Jordanian legislator must quickly realize this and take the very advanced and developed European experience and be guided by it to move to a safe digital environment through independent and special legislative texts in order to open the door in the field of digital investments and digital leadership through electronic banks and licensing them in Jordan. Here is the answer to the research question that addresses **the main question;** To what extent does the Jordanian Electronic Transactions Law conform to the rapid legislative developments in this sector in light of the transformation of international standards and the European Union to confront the emerging challenges of electronic banks.

I. 5. Responsibility Of The Electronic Authentication Service Provider In Jordan With Light Of The Provisions Of The Uncitral & EU Law Guidelines

[102] A. Hijazi, *E-Commerce*, Alexandria: Dar Al-Fikr Al-Jamia, (2003), p. 43, Cabrioli, "The Legal System of the State," accessed on 2 May 2023 at https://www.caprioli-avocats.com/.

This section delves into assessing the sufficiency of general regulations concerning electronic signature liability within Jordanian law and the necessity of developing specific regulations in this domain. It particularly considers the UNCITRAL Model Law on Electronic Signatures of 2001 and the European Directive on Electronic Signatures (1999/93/EC). The discussion revolves around the legislative responsibility in formulating directives and regulations, as well as endorsing digital signatures and validity certificates by service providers within the consumer protection framework. It emphasizes the importance of ensuring the continual safety of banking operations amidst technological advancements and the looming risks of financial fraud. On the other hand, "an electronic signature is a matter of confidence in the owner's ownership of the signature, and it can be difficult for the other contracting party to verify its authenticity, hence the importance of dealing with and regulating a digital signature".[103]

"The terms electronic authentication or electronic signature are used to refer to various techniques currently available on the market or still under development for the purpose of reproducing some or all of the functions identified as characteristics of handwritten signatures or other traditional authentication methods" in electronic environment.[104]

The notion of a "authorized party" The term "relying party" encompasses every entity that has the potential to depend on an electronic signature in the realm of cyberspace, in accordance with its designated meaning. A relying party can be any individual or entity, whether or not they have a contractual connection with the signatory or certification services provider. However, it is necessary that the certification services provider or the signatory itself be officially licensed and recognized by the government. Nevertheless, the expansive notion of a "affiliate" should not imply that the certificate recipient is required to authenticate the certificate issued by the certification service provider. [105]

Indeed, non-compliance with the requirements of Article (11) of the UNCITRAL Model Law pertains to the possible impact of the provision, which imposes a general obligation on the relying party to verify the electronic signature or certificate. The question arises when the

[103] Lukanova, Erika; Olsyakova, Miriam. Comparison of innovation in electronic banking of the largest Slovak banks. Marketing and management of innovations, 2022، Volume 13 Issue 4, pp. 1-9
[104] UNCITRAL, Enhancing Confidence in Electronic Commerce, Part I, Legal Issues Relating to the International Use of Electronic Authentication and Signature Methods, Vienna, 2009. p. 13.
[105] Mell, P. & Dray, J & Shook, J, (2019) *Unified identity management for a smart contract without third-party authentication services*, Bonn, p. 15.

relying party fails to meet the requirements of Article 11: should they be allowed to use the signature or certificate if a reasonable verification does not indicate that it is invalid? The conditions specified in Article 11 may need to be addressed in accordance with legislation that are beyond the jurisdiction of the UNCITRAL Model Law. Usually, this entails dealing with the repercussions that occur when the person depending on someone else fails to comply with these external legal obligations.

While developing the uncitral model law, it was suggested to distinguish between the legal framework that applies to the signatory and the certification service provider. Both parties should have specific obligations regarding their behavior if it conflicts with the electronic signature process. Additionally, there should be a separate framework that applies to the authorized party. The authorized party may find the Model Code of Conduct appropriate beforehand, but they should not be held to the same rigorous duties as the other parties.

However," the prevailing view was that the decision to create such a distinction should be left to the applicable law. It was also believed that basing civil liability of the service provider on the reasonableness of relying on the certificate of authenticity is necessary to balance providing protection to third parties and avoiding excessive obligations on the service provider".[106]

If it is unreasonable for a third party to rely on a defective notary certificate because of its past dealings with the certificate holder or because of the nature of the transaction, it is not reasonable to say that the notary services provider is liable in such a case, "when the purpose of the statutory requirement to sign is to provide assurance as to the integrity of the information to which it relates, and any change to that information after the time of signature may be detected".[107] The provider's responsibility for damages resulting from the electronic document may be nullified if any of the general liability rules apply, such as force majeure, actions of third parties, or the behavior of the injured party.[108]

---

[106] T. Kamel, "Electronic Documentation Service Providers (Legal Regulation, Duties and Responsibilities)," *University of Sharjah Journal of Islamic and Legal Sciences* 5 (2008), p. 237

[107] Article 6 UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, United Nations, New York, 2001.

[108] C. Lim, P.T. Futseng, A. Masri, O. Musa, MLM Kia, T.F. Ang, and R. Ismail, "Blockchain Technology Disrupted Identity Management and Authentication Service: A Survey," *International Journal of Advanced Sciences, Engineering and Information Technology*, Malaysia, 2018, p. 17.

The supplier's liability for the damage caused may be revoked if it can demonstrate that the damage was the result of an unforeseen event beyond its control and was caused by an uncontrollable cause. This is in reference to the decision to deny liability based on force majeure. The cause is exceptional and beyond the parties' control, provided that it is unforeseen and that the occurrence and damage of electronic devices used in electronic certification processes were the result of an earthquake, volcano, conflict, or flood.

"It is noted that these cases concern the non-liability of the service provider due to the actions of the customer holding the certificate or their decisions based on general liability rules. Therefore, the provider acted as a third party and not due to force majeure, which applies to damages arising for others despite the suspension or cancellation of the certificate at an irresponsible request".[109]

Similarly, if the certificate holder neglects to keep their password secure, fails to maintain the secrecy of their electronic signature, or does not inform the service provider that a third party has obtained or controlled the private key, or if the password is disclosed for any reason, it is the responsibility of the holder to notify the service provider so necessary precautions can be taken. Additionally, the holder must inform the provider of any modifications or changes to this data after the issuance of the certificate. The service provider's responsibility is voided if it is proven unreasonable for third parties to rely on the electronic authentication certificate, particularly if the certificate has been clearly marked as suspended or permanently canceled in the electronic certificate record maintained by the provider. This record must highlight any unreasonable reliance on the electronic certificate, thereby absolving the provider of liability.[110]

Article 8 of the European Directive on Electronic Signatures (1999/93/EC), titled "Liability," aims to determine the liability of electronic signature service providers for the services they offer. These providers are responsible for any damages caused by their services, whether to the signatory or any third party. This includes damages resulting from errors, omissions, or negligence in providing electronic signature services. However, the service provider's liability

[109] Hijazi, W**&**T, Kamel, *Electronic Signatures, Authentication Service Providers*, 2015. p. 11.
[110] J.C. Yorffy, A.F. Tappenden, and J. Miller, "Token-based Graphical Password Authentication," *International Journal of Information Security* (2011). pp.1-16.

is limited if the damage is caused by circumstances beyond their control or if the damage results from an act or omission by the signatory.

Article 8 also "requires Member States to establish procedures for the investigation and resolution of disputes related to e-signature services, which should be accessible, simple and inexpensive, and the European Directive on Electronic Signatures defines the liability of e-signature service providers and provides a framework for investigating and resolving disputes related to e-signature services".[111]

However," the European judiciary affected by the European Directive on Electronic Signatures has adopted a liability regime for electronic certification service providers, and the EU Directive on electronic signatures already requires foreign certification service providers to comply with both their original data and EU regime, which is a higher standard than accredited certification service providers in an EU member".[112]

Article (8) of the Jordanian electronic transactions law No. 85 of 2001, as amended, obliges authentication service providers and electronic service providers to take the necessary measures to preserve the reliability and legitimacy of electronic transactions through the use of electronic signatures, digital certificates, encryption and electronic authentication of transactions, in accordance with the controls and conditions determined by the executive authority. The regulations of the law [113] aim to promote the safe and reliable use of electronic technologies in commercial and legal transactions, as well as to encourage e-commerce and investment in countries. The law aims to promote the safe and reliable use of electronic technologies in commercial and legal transactions, and to encourage e-commerce and investment in countries[114]. The law also guarantees equality between electronic and paper-based transactions in terms of law and evidence and protects the rights of consumers and contracting parties in electronic transactions.[115]

---

[111] Article 8 of the European Directive on Electronic Signatures (1999/93/EC).

112 The European Court of Justice rules on the liability of banks for unauthorized low-value transactions using contactless payment, Library of Congress (December 21, 2020).

[113] Article (8) of the Jordanian Electronic Transactions Law No. 85 In 2001.

[114] Barba, Robert. American banker, the battle for talent rages as electronic banking becomes paramount to paramount importance. 17/8/2016, Volume 181 Issue 158, p. 1.

[115] Article (34) of the Jordanian Electronic Transactions Law stipulates the following: It must be a certificate Documents showing the identification code shall be approved in the following cases: a- It must be issued by an authorized or accredited body. Issued by a licensed authority from a competent authority in another recognized

In fact, through this article, it is possible to emphasize the need for specific provisions in Jordanian legislation to regulate the work of notary bodies and address the civil liability resulting from their failure to perform their duties. The general provisions of liability in the Jordanian Civil Code or the Electronic Transactions Law are insufficient to provide effective protection for those affected by the electronic documentation process. These texts may not adequately determine the liability of electronic authentication service providers, as Jordanian law does not specify how the documentation process should be conducted or the obligations arising from it.

Herein, the lack of compatibility and harmony between Jordanian laws and the European legislation mentioned above cannot be denied. Through this, the Jordanian legislator must quickly realize this and take the very advanced and developed European experience and be guided by it to move to a safe digital environment through independent legal and legislative regulation, especially for electronic banks that face regulatory challenges and cyber threats in order to open the door in the field of digital investments and digital leadership through electronic banks and their licensing in Jordan. Here is the answer **to the research question** that addresses the main question: To what extent does the Jordanian Electronic Transactions Law conform to the rapid legislative developments in this sector in light of the transformation of international standards and the European Union to confront the emerging challenges of electronic banks.

In addition to, for answering to **the second sub-question** of the research about what are the weaknesses included in the Jordanian Electronic Transactions Law in light of the international model and European Union directives" They do not exist. There are specific, independent and advanced editorial exclusivities that keep pace with advanced European legislation, which enables the digital gaming market in Jordan to move to the stage of establishing banks that are fully and independently electronically powered. After one of the shortcomings in Jordanian law, which answers the second question, which is called the research.

The Jordanian legislator seems to have overlooked the gaps in the legislation concerning many aspects of the electronic authentication process, such as defining the process of authenticating

country. Issued by a legally authorized government department, institution or body. d- Issued by an authorized body the parties to the transaction for approval.

an electronic signature, the essential data required in such certificates, the responsibilities arising from them, and the obligations of the provider to activate electronic [116] transactions.[117]

Since most of the obligations of the electronic certification authority are more about exercising due care rather than achieving specific results, the requirement for an injured third party to prove their reliance on the notary certificate due to the negligence of the notary authority constitutes a practical obstacle in determining the legal liability of that authority. Some obligations of an electronic certification entity are technical in nature, making them difficult for others to understand and thus challenging to prove. Therefore, it can be argued that there should be a presumption of error by the notary authority, which would shift the burden of proof to the notary authority to demonstrate that it did not breach any of its legal obligations.[118] However, we also believe that the notary authorities should not be held legally liable if it is unreasonable for others to rely on the certificate of authenticity.

The researcher believes it is crucial for the Jordanian legislator to prepare a precise legal framework with clear provisions to create a stable investment environment in Jordan for potential investors. In the alternative, they may encounter ambiguity regarding the legal nature of liability, the conditions for its establishment, and the resulting repercussions. Presently, the Jordanian legislator has not addressed these points within a specific legal framework, which has raised concerns regarding liability. Specifically, the service provider's liability for damages resulting from defects in the electronic authentication process and the customer's responsibility for violations related to the certificate are at issue.

Consequently, the service provider is contractually responsible for any breach involving the creation or use of data without the customer’s consent. The provider is also obligated not to delete, add, or modify personal data as per Article (8) of the European Directive on Electronic Signatures, if such data is necessary for the delivery and preservation of the certificate.

---

[116] T. Amer, Vladislav Yevseyev, Ayman Amer, Natalia Dimska, Ashish Karr Lohash, and Vyacheslav Lyachenko. "*Electronic User Authentication Key for HMI/SCADA Access via Unsecured Internet Networks*." Faculty of Computer Science and Information Technology, Ajloun National University, Ajloun, Jordan, 2022. p. 14.

[117] The paper describes a way to ensure secure electronic authentication for users accessing human-machine interfaces (HMI) or supervisory control and data acquisition (SCADA) systems over insecure internet networks HMI/SCADA systems are commonly used in industrial environments to monitor and control complex processes, and their security is a serious concern given the potential consequences of unauthorized access or malicious attacks.

[118] Abu Al-Lail Al-I, *Documenting Electronic Transactions, Burning, Nature and Legal Impact*, 2018.p.17.

Article (8) highlights the inadequacy of general rules in regulating this responsibility, necessitating the Jordanian legislator to enact specific legal provisions to delineate the obligations of notary service providers and the legal nature of their responsibility. This should be done while achieving legal balance by requiring reasonable reliance on electronic authentication certificates. Given that the Jordanian legislator has not addressed this topic in light of the challenges and difficulties faced by researchers, they have resorted to comparing and analyzing international legislation to gain a clearer understanding of subsequent needs.

In the event that consumers are interested in participating in electronic signature activities, they may confront a legal vacuum and instability regarding the conditions for its establishment, the associated consequences, and legal liability. Jordan's legislator has not expressly addressed these points within a legal framework that is specific, detailed, and comprehensive, and that is capable of accommodating all potential developments in the swiftly evolving field of e-commerce. This lack of clarity raises concerns regarding liability, such as the accountability of customers for certificate violations and the responsibility of service providers for damages that result from deficiencies in the electronic documentation process.

The researcher emphasizes the necessity for the Jordanian lawmaker to acknowledge the importance of promoting legislation, namely in the fields of information technology and financial transactions. Continuous improvement is required in these areas to coincide with the path of global e-commerce, reduce legal difficulties, and utilize the European experience as a catalyst for creating accurate and essential laws while addressing any ambiguity. Legal stability enhances the trust of e-commerce investors, pushing their development. Additionally, the service provider is required to refrain from deleting, keeping, adding, or altering the personal data that is necessary for delivering or maintaining the certificate. Nevertheless, the possibility of restricting or eliminating the legal responsibility of the service provider is still questionable. Consequently, the service provider is legally obligated to take responsibility for any violation related to the creation or use of data without the explicit agreement of the consumer.

Chapter II

Challenges Facing Electronic Financial Operations

The provides chapter an introduction to an explanatory review of electronic banks, comparing them with conventional banks, highlighting their differences, advantages, and disadvantages. The research relies on concepts within the framework of Jordan and the international community to illustrate the variances between traditional banks and electronic banks, the personal benefits for customers and investors, and their impact on the national economy. aims to clarify the main risks and threats faced by electronic banks, where the first chapter discussed the issue of electronic documentation and its importance in light of the potential risks to determine the aspects of responsibility of parties associated with electronic financial operations through electronic banks and parties and their responsibilities as a new experience

Therefore the second chapter hrerin, will finalize the research by examining the practical application of electronic banking, emphasizing key aspects such as electronic payment methods, technical and criminal protection of electronic banking operations, and the vulnerabilities banks face in money laundering activities. This will help to define the challenges confronting electronic banks. The focus will be on analyzing the legal regulatory frameworks in Jordan and European approaches, as outlined in EU charters, directives, and judicial precedents. Additionally, the chapter will explore the influence of international law within the framework of the open method of cooperation to enhance the formulation of Jordanian transaction law regulations.

The research highlights the importance of adhering to global standards and the need for more robust regulatory requirements to ensure the security and stability of electronic payment systems. By focusing on strengthening legal regulations, and creating a secure and resilient digital financial ecosystem that fosters innovation while protecting all parties involved. This

balance between security and growth is essential for the continued success and trust in electronic payment methods.[119]

In fact, the landscape of electronic payment risks is complex. The risks associated with electronic payments can be categorized into several critical areas. Each of these categories poses unique threats, which, if not addressed through legal regulations, could undermine the confidence and stability of the digital economy.[120]

On the other hand, setting clear expectations for security measures, these regulations help protect consumers and businesses, ensuring that electronic payment systems remain secure and trustworthy.[121]. In addition to local regulations, international standards and frameworks such as the Payment Card Industry Data Security Standard (PCI DSS) that provide guidance for securing payment card data, compliance with these standards helps protect payment systems on a global scale.[122]

The chapter will look for a detailed analysis of the payment system issued by the EU [123], which is for example advanced and modernized, and to serve as a motivation and guidance tool for the Jordanian legislator to implement appropriate ones in Jordan.

II.1. Managing Risks Facing Electronic Payments

The first step of the framework aims to confirm that the payment activities performed by the entity qualify as payment services. Identifying these activities aids in creating effective control and supervision frameworks, preventing unnecessary overlap and duplication of regulatory

[119] Z. Kalinek, F. Marienkovich, S. Molinello, and F. Liébana-Cabanillas. "A Multiple Analytical Approach to Predict Peer-to-Peer Mobile Payment Acceptance." *Journal of Retailing and Consumer Services* (2019), p. 13.

[120] Zhang, L. Understanding the impact of financial incentives on NFC mobile payment adoption: an empirical analysis. Int. J. Bank Mark. 2019. p. 37.

[121] European Banking Authority. (2018). The text refers to regulatory technical standards (RTS) that relate to strong customer authentication (SCA) and shared and secure communications (CSC) as set out in the Second Payment Services Directive (PSD2), https://www.eba.europa.eu/ . It reaches the value of October 17, 2023.

[122] The source is the Payment Card Industry Security Standards Council (PCI SSC) in 2020. The current version of the PCI Data Security Standard (PCI DSS) is 4. https://www.pcisecuritystandards.org/ . Reaches the value of October 20, 2023.

[123] The "Revised Payment Services Directive" (PSD2), formally known as Directive (EU) 2015/2366 on payment services, is a large EU regulation aimed at modernizing and standardizing the legal structure of payment services within the EU.

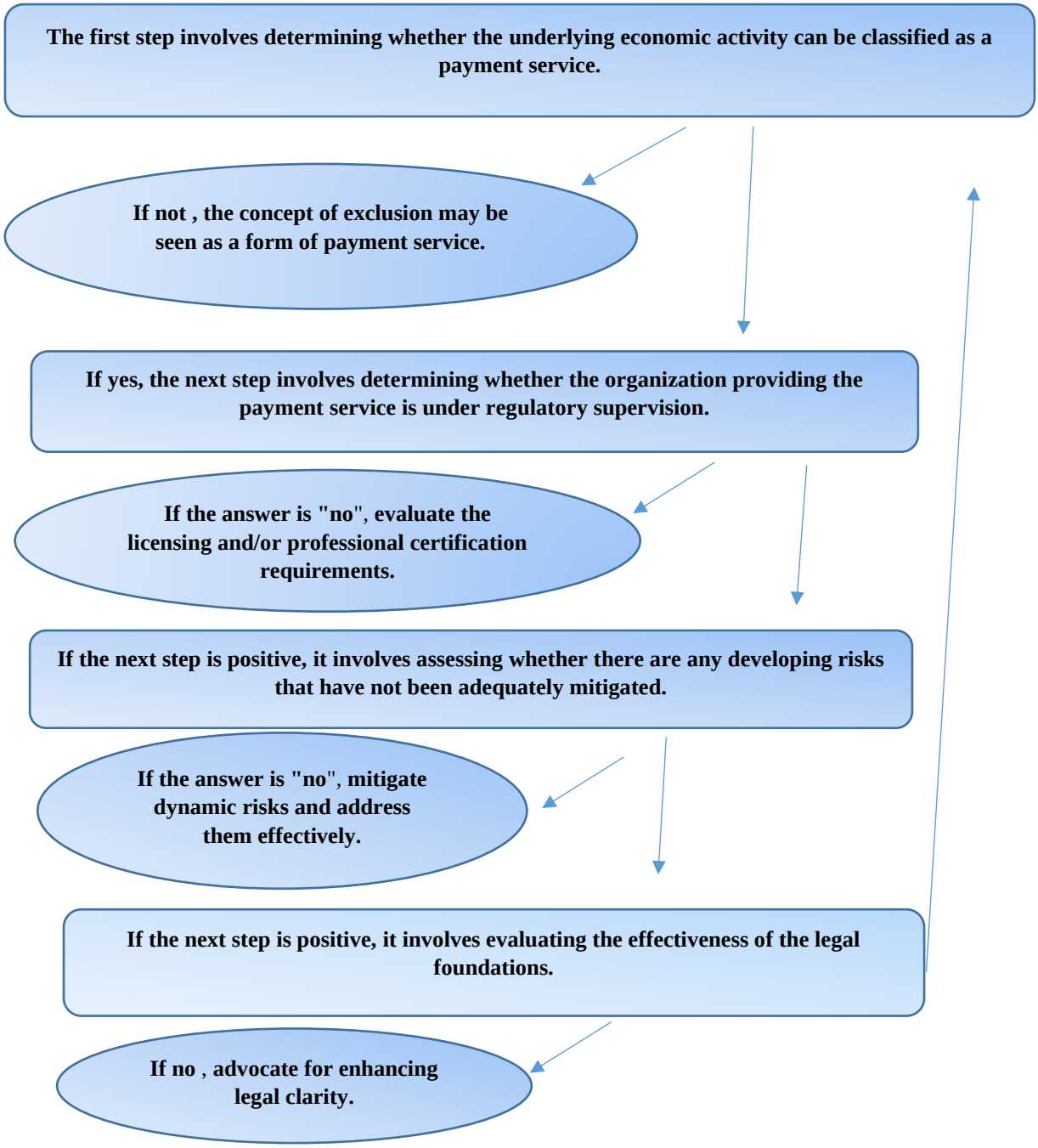
efforts. International experience suggests that regulated activities can include e-money issuance, local and cross-border money transfers, merchant acquisition services, and digital payment codes. These activities mainly pertain to services offered to users of the payment service rather than focusing on payment systems themselves. This list is not exhaustive and can vary depending on the jurisdiction.

Clear and explicit legislation regarding payment services serve to offer clarity about the actions involved. Article 4(3) of the updated EU Payment Services Directive (PSD2) defines payment services as any commercial activity related to eight specific activities outlined in the Directive.[124]

The Jordanian legislature has defined an electronic payment system as a set of programs or tools designed to pay, transfer, clearing or settle funds electronically and approved by the Central Bank.[125] According to the definition of the Jordanian legislator, payment services are the procedures related to the issuance and management of any payment instruments or electronic transfer of funds included in the provisions of this system.[126] Certain payment operations may be exempted from the Payment Service Rules. According to Article 3 of PSD2, it explicitly states that it does not apply to 15 specific payment activities. These activities include cash transactions, paper payment instruments like as checks, drafts, vouchers, and money orders, as well as ATMs that provide cash withdrawal services within the EU.

[124] Revision of Directive (EU) 2015/2366 on payment services.
[125] Jordanian electronic payment and transfer system for funds in 2017.
[126] Ibid., p. 8.

Figure No. (5); Illustrates the analytical framework used to organize payments.[127]



Source: The official website of the Central Bank of Jordan.

[127] Central Bank of Jordan, Control and Control Department on the National Payment System, Sixth Annual Report, 2021.

II. 1.1. Electronic Payment Codes

This is a novel approach that utilizes digital codes for conducting financial transactions. Nevertheless, the technique has not undergone extensive testing. The introduction of stable crypto assets, which have a fixed value linked to a certain group of assets, aims to overcome the limitations of prior crypto assets.

Moreover, global stablecoins, commonly referred to as GSCs, have the capacity to enhance cross-border payment systems that have been expensive, sluggish, lacking transparency, and divided. It is imperative to address several regulatory concerns and dangers associated with crypto assets and their potential global stablecoins (GSCs). Although crypto assets can be linked to payment methods or stores of value, they may also exhibit characteristics similar to stocks or commodities. Regulatory gaps may occur when these assets are situated beyond the jurisdiction of market regulators and the payment system.

The concept of supervision refers to the process of monitoring and supervising activities to ensure compliance, and potential global stablecoins (GSCs) have posed different challenges across different domains, the challenges encompass various aspects such as ensuring legal clarity, establishing effective governance and investment regulations, maintaining financial integrity, enhancing the safety and efficiency of payment systems, addressing cybersecurity concerns, promoting operational flexibility, ensuring market integrity, safeguarding data privacy and portability, as well as protecting consumer and investor interests and ensuring tax compliance. It is crucial to thoroughly evaluate the possible benefits and drawbacks of digital payment codes in relation to public policy goals.

In the United States, there has been a deliberate examination of several factors, including the amount of physical currency in circulation, the status of the reserve currency attributed to the US dollar, the flexibility of the banking system, and the accessibility of digital payment alternatives.[128]

[128] L. Brainard. "Digital Currencies, Stablecoins and the Evolving Payments Landscape," notes on the future of money in the digital age, Washington, D.C., October 16, 2019, available at: https://cutt.us/ZJZEv (accessed October 22, 2023).

The broader implications include several aspects such as protecting investors' interests, ensuring consumer protection, addressing data privacy concerns, managing systemic risk, influencing monetary policy, and protecting national security. Several jurisdictions, including Singapore, Switzerland, and the USA, have implemented legal reforms in response to the emergence of digital payment codes as a medium of exchange.[129]

On February 2015, The World Bank recommended that the Central Bank of Jordan revise the legal framework governing the administration and operation of payment systems. In order to enhance the governance of the financial system, the World Bank has advised that the Central Bank of Jordan should separate its operating and supervisory roles. This would enable the bank to operate as a regulator, supervisor, and driver of innovation in the payments value chain. The development of JOPACC commenced on January 16, 2017. The central bank of Jordan reached an agreement with 25 banks. The objective in the Kingdom is to establish the "Jordan payments and clearing company".[130]

For example the risk of defrauding the Customer in any payment transaction, the Customer is exposed to the risk of fraud and theft when he discloses his financial information and/or credentials. This is exacerbated by the payment withdrawal model, where customer information passes through third-party systems. For this reason, with JQR, JOPACC has committed to only allowing or requesting payments. This means that the customer will not disclose any of their payment credentials to the merchant, and instead will only direct their financial institution to debit their account and merchant credit. By adopting the payment or request form for payment, JOPACC has significantly reduced the risks associated with customer fraud in a QR-enabled payment system.[131]

This is indeed what **the main hypothesis** of the research indicates and confirms the validity of "on which the research is based, which states the following " legislation has been implemented

[129] Cristiano, J.C., J. Ehrentraud, and M. Fabian. "Big Tech Companies in Finance: Regulatory Approaches and Policy Options." *FSI Summaries* No. 12. Basel, Switzerland: Bank for International Settlements, 2021, Available from URL: https://www.bis.org/fsi/fsibriefs12.pdf. (accessed January 13, 2023).

[130] JOPAC. The company, which was founded in 2017, is presently owned by 22 banks and the Central Bank of Jordan, as well as all 25 commercial banks in Jordan at the time of its establishment. Its capital is 12 million Jordanian Dinars. Its clients are commercial institutions and payment service providers that establish connections with JOPACC payment systems in order to offer financial services to their clients, who are end users. JOPACC maintains five payment systems in its portfolio.

[131] Guide on Common QR Code Standards for Payments in Jordan, JOPACC, 2022.

to limit identity theft and fraud in online banking. However, authorities are encountering challenges in establishing secure and authenticated digital identity procedures. New laws have been introduced to protect electronic bank customers, ensuring transparency in fees, conditions, and dispute resolution systems"

Indeed, the researcher believes Jordan has made significant progress in the payment system and its protection by establishing a subsidiary of the central bank and other banks tasked with monitoring payments, regulating them, and keeping abreast of global developments in this field. However, simultaneously, the Jordanian legislator faces clear deficiencies at the legislative level of the payment system. This is indeed what I have raised in the second sub-question, which refers to this is indeed what I have raised in the second sub-question, which refers to**, the second sub-question** "what weaknesses does the Jordanian Electronic Transactions Law include in light of the international model and directives of the European Union"; there is a need for the legislature to actively engage in researching, analyzing, and comparing international laws that have developed this important sector. This is particularly crucial in light of the COVID-19 pandemic and the increasing trend towards electronic payments.

II. 1.2. Risk Screening And Management

Fraud detection and prevention are paramount to safeguarding the security and integrity of online payment systems. Below is further insight into the pivotal role that fraud detection systems and artificial intelligence (AI) play in identifying suspicious activity and thwarting fraudulent payments. These systems are specifically engineered to identify and prevent fraudulent activities, employing sophisticated algorithms and software units that continuously monitor transactions for indicators of fraudulent behavior.

Their approach encompasses the utilization of rules-based systems, anomaly detection, and machine learning algorithms to detect patterns or unusual behaviors. Artificial intelligence, particularly machine learning, proves to be an invaluable asset in spotting and thwarting fraudulent activities. It possesses the capability to adapt and acquire knowledge from historical data to pinpoint new and evolving fraud patterns. AI models excel in swiftly scanning large volumes of data in real-time, enabling them to accurately pinpoint suspicious transactions. This renders them exceptionally effective in preventing fraud.

Machine learning models may use transaction data to identify distortions by analyzing several characteristics such as transaction amount, frequency, location, and other factors. Natural language processing (NLP) can be used to scan text data for indications of fraudulent activity, such as in email correspondence or chat conversations. [132]

This can facilitate deep learning to detect complex patterns that may be difficult to distinguish using traditional techniques, such as real-time monitoring. Fraud detection systems and artificial intelligence operate in real-time, enabling immediate intervention when any suspicious activity is detected. The use of real-time monitoring enables rapid intervention or screening of potential fraudulent transactions. Fraud detection systems may be designed according to the exact requirements of the organization or payment platform. They have the ability to adapt to emerging deception techniques.[133]

Conversely, a critical obstacle in detecting fraud is to minimize the incidence of false positives, which refer to legitimate transactions that are mistakenly identified as fraudulent. AI enhances accuracy and reduces the occurrence of false alarms. Many companies and financial institutions collaborate to share data and knowledge on the development of fraud tendencies, thereby improving their fraud detection capabilities together.

It is important that fraud detection systems continuously enhance their capabilities as they handle larger amounts of data and gain knowledge from their past encounters. This enhances their effectiveness over time. Robust fraud detection and prevention technologies are critical to protecting online payment systems and maintaining user trust. It is a critical component of the broader endeavor to ensure the safety of online transactions and prevent financial losses and damage to an individual's reputation resulting from fraudulent behavior.

This is confirmed by the most important **hypotheses** on which the research was based, which state that, there is an inverse relationship between assessing potential systemic risks associated with electronic banks and developing risk management procedures to ensure financial stability amid the growth of the cyber insurance market, and regulation to reduce risk.

---

[132] M. Serafi, *Management of Banking Operations - Ordinary - Exceptional - Electronic*, 2nd ed. (Egypt: Dar Al-Fagr for Publishing and Distribution, 2016). p. 12.

[133] Henry H. Perritt, jr.*Regulatory models for protecting privacy in the Internet*", Faculty of Law of Villanova University https://www.ntia.gov/ (accessed June 5, 2023.)

In fact, both EU & UN have consistently developed legal regulations and recommendations to prevent fraud and maintain financial security, and the EU largely emphasizes regional standards and directives, while the United Nations primarily addresses international frameworks. Payment services legislation 2 (PSD2) is an influential EU legislation that has a significant impact on online payment transactions. It requires strong customer authentication (SCA) and calls for secure online payment mechanisms. In addition, it places great emphasis on preventing fraudulent activities and managing potential risks.[134] This includes implementing regulations to ensure secure communication between payment service providers and their customers. Furthermore, the GDPR focuses primarily on protecting data privacy, but also has implications for online financial transactions. Organizations dealing with payment data must ensure that they comply with the strict data protection rules outlined in the GDPR in order to protect sensitive customer information. European law was comprehensive and implemented rapid and constantly evolving measures. As an illustration, consider the rules regarding anti-money laundering (AML). The European Union implements anti-money-laundering directives with a view to combating money-laundering and the financing of terrorism. Financial institutions and payment service providers should establish robust KYC (Know Your Customer) processes and systems to identify and report potential illicit transactions in accordance with these requirements.[135]

Conversely, the United Nations Convention against Corruption (UNCAC) is one of the structures and regulations that the United Nations provides. The United Nations Convention against Corruption (UNCAC) is an international convention that is explicitly designed to combat corruption, a phenomenon that is closely associated with financial fraud. A variety of measures are incorporated into the Convention to prevent and combat corruption in both the public and commercial sectors.

While fraud has not been explicitly discussed, these measures encourage prudent financial behavior and openness, and include UN laws and principles on consumer protection, as they include guidance on consumer protection. These principles extend to online payment systems, ensuring that consumers are treated fairly and protected from fraudulent activities, particularly

[134] European Central Bank (ECB) Occasional Paper Series No. 223/22 May 2019.
[135] Revision of Directive (EU) 2015/2366 on payment services.

in the area of e-commerce, despite any potential restrictions. Although it is not legally enforceable, it serves as the basis for national governments.[136]

The following table No. (1); Displays a risk map that classifies payment actions based on their potential impact.[137] in the course of this discussion, the abbreviations H, M, and L represent high, moderate, and low, respectively.

Payment Service	Protection Of Funds	Financial Integrity	Cybersecurity &Data Security	Access To Payment Systems	Interoperability
Account Issuance Services	M	H	H	L	M
Issuing Electronic Money	H	L	M/H	M	L
Transfer Money Locally	H	H	M/H	H	L
Cross-Border Money Transfer	H	H	M/H	H	L
Merchant Acquisition Services	H	L	M/H	M	M
Digital Payment Token Services	M	H	M/H	H	L

Source: The official website of the Central Bank of Jordan.

This detailed analysis allows to evaluate the evaluation of the advantages and disadvantages of each payment service based on several factors. It is important that the choice complies with special criteria and details, based on the type of transactions and financial services desired by the customer. The protection of funds relates to the protection of funds within the system. Services marked "high" usually offer improved security measures in this regard. Financial integrity refers to the reliability and credibility of financial transactions. The term "high" refers to a strong degree of financial integrity, while cybersecurity and data security are about protecting data and systems from cyberattacks. The term "high" refers to strong security measures, while access to payment systems refers to the service's ability to integrate seamlessly

[136] United Nations Guidelines for Consumer Protection (as expanded in 1999), Department of Economic and Social Affairs, United Nations, New York, 2003.
[137] Central Bank of Jordan, Control and Control Department on the National Payment System, Sixth Annual Report, 2021.

with existing payment systems. The term "high" refers to excellent accessibility. Interoperability is the ability of a service to work seamlessly with other systems. The terms "moderate" or "low" refer to different levels of compatibility.

In doing so, individuals may make informed judgments about which payment services are most appropriate for particular use cases. If you value strong financial integrity and the ability to use payment methods, a "local money transfer" may be a good option. Alternatively, if you want improved collateral for your money and strong cyber and data security measures, Digital Payment Code Services may be a more convenient option. The decision depends on your own needs and preferences in each area.

The previous table shows the levels of money protection and financial integrity of electronic banking and electronic payment operations and the level of these operations in terms of rise and fall. The scope of cybersecurity, information security, access to payment systems, and interoperability, where it was found that electronic banking and electronic payment operations are all subject to rise and fall in the level of risk depending on the variables available in each electronic transaction and in each electronic bank or community, the electronic environment and means of protection. In order to meet the need for cash of customers and limited assets available for repayment in the event of the insolvency of the trustee or bank.[138]

It is important to recognize that placing client funds in a segregated bank account by an electronic non-bank source of funds only provides protection against the bankruptcy of that non-bank source. However, it does not extend to protecting funds from the insolvency of the bank responsible for keeping them. It is important to ensure the protection of transient funds. These funds refer to the amounts of cash received by the payment company from the user for the supply of products or services, which have not yet been disbursed to the intended recipient. It does not include Transitory funds Money derived from payment.[139]

The design of the payment system must take into account many of the procedures involved in the settlement, such as those observed in the cheque clearing system. In the context of merchant

[138] GSM Association (2016) "Mobile Money Protection: How Service Providers and Regulators Can Ensure Customer Money Protection", p. 8.
[139] J.C. Laguna de Paz, (2023), *Some Implications for the New Global Digital Economy of Financial Regulation and Supervision*, Journal of Banking Regulation, p. 11.

acquisition and money transfer, the concept of transient funds presents the possibility of credit risk especially when a payment service provider (PSP) holds consumer funds at any stage of the payment process. Although it is costly for payment service providers (PSPs) to immediately transfer payments to the intended recipient, it is not uncommon for there to be a delay of a few days before the beneficiary has actually received the funds.

In some cases, the amounts of money earned and at risk may be significant, such as money raised by a postal service agent. In order to enhance customer safety, it is recommended that regulators impose protective standards on client funds collected by these companies, similar to those applied to electronic money.[140]

Hence, the researcher believes that financial deposit insurance is a regulatory measure that expands the coverage of bank deposits, as stipulated in the current deposit insurance legislation, to include assets held in stored value facilities, i.e. electronic money. This particular strategy ensures the protection of consumer funds stored in non-traditional means of access. This technique has also been examined in other countries. However, insurance for pass-through deposits depends on the current legislative definition of "deposits" and the fulfillment of certain requirements, including the formation of guardianship relationships, the authentication of identities and the exact amount of funds held by each individual owner. These standards help establish functional equivalence among similar services that possess deposit features, making them suitable for inclusion in the deposit insurance program. The client's funds are likely to be protected by an insurance policy or similar guarantee provided by an insurance company or credit institution.

It is not recommended that these warranties belong to the payment institution concerned. The quantity should be proportionate to what would have been avoided had the insurance policy or similar security not existed. The payment institution is obliged to make the payment in the event of its inability to meet its financial obligations. Reserve requirements imposed by central banks have been used as a measure to mitigate the potential risks associated with the high concentration caused by large non-bank payment service providers (PSPs).[141] Non-bank

[140] For clarification, see Article 10 on the safeguarding requirements of Private Sector Strategy 2.

[141] Payment service providers (PSPs) are entities that oversee and deal with electronic payments for businesses and individuals. They act as intermediaries in transferring payments from payer (consumer) to payee (merchant or

payment service providers (PSPs) have been tasked with maintaining reserves in order to ensure the protection of customer funds, particularly in areas where the use of mobile payments has become prevalent. The scope of implementation of some of the rules by the central bank of Jordan has gradually been extended to prominent technology companies operating as non-bank payment institutions. From January 2019 onwards, it became mandatory for these companies to keep all customer funds in a reserve account with the central bank of Jordan, without Accumulation of any income. Prior to this, a series of regulations were instituted in January 2017, which required non-bank payment institutions to maintain 20% of customer funds in a segregated premium custody account at a commercial bank. Subsequently, in January 2018, this percentage was elevated to 50% [142].

II.1.3. Financial Integrity

Financial integrity refers to adherence to ethical and moral principles in financial matters, and ensuring transparency, honesty and accountability in payment goods and services has the capacity to be employed as instruments for the financing of terrorist activities and the laundering of illicit funds. Therefore, it is imperative to implement AML/CFT regulatory standards to ensure the financial integrity of payment transactions. The Financial Action Task Force (FATF) has compiled a document titled "Guidance for a risk-based approach: prepaid, mobile, and online payments" to offer countries guidance on the effective implementation of anti-money laundering and combating the financing of terrorism (AML/CFT) measures using a risk-based strategy. [143]

As a result, regulatory surveillance is essential to guarantee that e-banks adhere to the relevant rules and regulations and maintain the confidence of the public. E-banks must collaborate with regulatory authorities to comprehend and adhere to the expanding regulatory environment in order to safeguard their customers' financial information, as well as invest in sophisticated security measures and compliance systems. Electronic this phenomenon also confirms my **hypothesis**" electronic banks will face difficulties in complying with several financial rules,

service provider). Payment Service Providers (PSPs) offer a range of services and technology that facilitate secure, fast and easy online transactions.

[142] Central Bank of Jordan, Control and Control Department on the National Payment System, Sixth Annual Report, 2021.

[143] Financial Action Task Force "Guidance for a risk-based approach to prepaid cards, mobile payments and online payment services", Paris, available at: https://cutt.us/NqO3S (accessed April 15, 2023).

such as anti-money laundering (AML) and know-your-customer requirements, and the need to develop comprehensive strategies to manage their transaction scenarios. "

The researcher believes that countries face limited discretion in formulating AML/CFT measures because of their commitment to comply with the global normative framework. Risk-based guidelines, such as those published by the Financial Action Task Force (FATF), are intended to assist countries in reducing the risks associated with particular goods or services by formulating focused and tailored supervisory, regulatory and/or executive procedures, and the user text does not provide any information for rewriting.

Jordan has implemented laws, including the Anti-Money Laundering and Combating the funding of Terrorism Act No. 46 of 2007, to tackle the problems of money-laundering and terrorist funding within its legal framework. The objective of this rule is to guarantee adherence to global standards and commitments in particular, defined domains. Jordan has created a finance division known as the Anti-Money Laundering and Combating the Financing of Terrorism Unit. The primary responsibility of the Anti-Money Laundering Unit is to receive, analyze, and distribute reports pertaining to suspicious transactions, money laundering, and terrorist funding. [144]

However, in Jordan, financial organizations, particularly banks, are required to do customer due diligence (CDD) in order to authenticate the identities of their clients, evaluate the potential for money laundering or terrorist funding, and maintain transaction records. Jordanian financial institutions must inform the Anti-Money Laundering Unit about any transactions that raise suspicions. Reporting is of utmost importance in the AML/CFT framework.

The Financial Action Task Force (FATF) has also promoted international recommendations to regulate virtual assets (VAs) and virtual asset service providers (VASPs) in order to protect financial integrity.[145] The Financial Action Task Force (FATF) defines "virtual asset" as digital representations of value that are tradable, transferable, and can be utilized for payment or investment. This include digital representations of value that function as a means of facilitating

[144] Law No. (46) of 2007 on the Anti-Money Laundering Law, published in the Official Gazette in Volume No. (4831) dated 17/6/2007 on page No. (4130) as amended by Law No. (31) 2015.
[145] Financial Action Task Force. "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." Paris, 2019. p. 7.

transactions, a standard measure for assessing worth, and/or a means of preserving wealth. Virtual assets fundamentally vary from fiat money, which is the officially recognized currency of a country that is accepted as a form of payment. If a virtual asset service provider (VASP) falls within a product or service category or engages in an activity that is governed by the Financial Action Task Force (FATF) standard, it is obligated to adhere to the Anti-Money Laundering and Terrorist Financing (AML/CFT) criteria. This requirement is applicable regardless of the level of risk posed by VASP in a particular country, with the exception of transactions below $1,000, which are free from customer due diligence. It is imperative that all Virtual Asset Service Providers (VASPs) get anti-money laundering/combating the financing of terrorism (AML/CFT) supervision that is appropriate for the specific features, scale, and susceptibilities of their activities. The FATF mandates that nations must implement specific anti-money laundering and countering the financing of terrorism regulations that are rooted in activities. The ongoing development of the risk-based technique considers the specific attributes, magnitude, and possible hazards linked to certain activities. The European Union (EU), United Kingdom (UK), and Jordan have adopted a system based on thresholds to determine the necessity of implementing Know Your Customer (KYC) rules.[146]

This technique involves analyzing the amount of money laundering and terrorist financing risks associated with payment service providers (PSPs) by considering factors such as account balances and transaction volume. The term "electronic money" includes a wide range of definitions. However, it should be noted that some e-wallets, commonly referred to as e-wallets, may have limited access, use, and functionality. In light of this, there is a possibility that these specific e-wallets may present less risk in terms of laundering Money and terrorist financing. Thus, some countries may choose to exempt these e-wallets from regulatory measures[147]. In Jordan, reporting organizations are subject to AML/CFT obligations, regardless of whether the transactions involve fiat currencies or digital symbols.[148]

[146] ECB Occasional Paper Series No. 223 / May 2019.
[147] IMF and World Bank (2019) "FinTech: Experience to Date," IMF Policy Paper, IMF, Washington, D.C., available at: https://www.imf.org/ en/Publications/Policy-Papers/Issues/2019/06/27/ Fintech-The-Experience-So-Far-47056 (accessed September 11, 2023).
[148] Cyber Risk Adaptation Instructions issued by the Central Bank of Jordan in 2018.

II. 1.4. Data And Cybersecurity

Today, new payment models and new participants not only boost competition and innovation, but also introduce new cybersecurity and data security vulnerabilities. Open banking, where payments account infrastructures are provided to payment service providers (primarily banks) accessible to non-bank PSPs, can be a major concern.[149]

This facilitates the development of new payment services, such as account information and payment start-up services offered by ELMIs and PIs, but may also increase the risk if third-party non-bank payment service providers fail to meet security requirements. In addition to protection against fraud and operational disruptions, this risk management is essential to maintain data privacy. Protecting public trust in payment services is critical from a central banks' perspective.[150] The escalation of incidents may have a negative impact on public trust and put authorities at risk to their reputation. To protect data privacy, This is confirmed by the most important **hypotheses** on which the research was based, which state that" Regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system.

The EU General Data Protection Regulation ensures the safeguarding of individuals in regards to the handling of their personal data and its free flow. Both bank and non-bank payment service providers must adopt controls and provide sufficient risk management to effectively handle cyber hazards. These areas are of utmost importance, particularly in regards to user authentication, data loss protection, and the detection and prevention of cyberattacks. Technology hazards primarily pertain to the possibility of payment services becoming vulnerable and the dangers linked to insufficient IT management by service providers. To mitigate risks, it is necessary to prioritize IT security measures, including virus protection, software upgrades, and data backup. Technology risk management concepts encompass the implementation of a strong and dependable framework for managing technology risks. This involves improving the security, dependability, resilience, and recoverability of systems. Additionally, it entails employing robust authentication procedures to safeguard consumer

[149] Basel Committee on Banking Supervision (2019) "Report on Open Banking and APIs", November, available at: https://www.bis.org/bcbs/publ/d486.htm (accessed May 17, 2023).
[150] European Central Bank (ECB) Occasional Paper Series No. 223/22 May 2019.

information, transactions, and systems. To improve cybersecurity and data security, organizations can utilize technological standards and guidelines that are essential for meeting licensing requirements and regulatory compliance. The current international guidelines on cyber resilience have mostly emphasized its implementation in financial institutions, since they have more significant systemic consequences. However, payment service providers have received comparatively less attention in this regard.[151]

Nevertheless, a number of jurisdictions have developed distinct national guidelines to address these issues. Jordan has enacted technology risk management guidelines and electronic hygiene regulations that apply to all licensees involved in providing technology payment services.[152] The European Commission has entrusted the European Banking Authority (EBA) with responsibility as set out in PSD2 (Article 98), for the development of regulatory technical standards governing open and common communication channels between payment service providers (PSPs), including those that facilitate account service, payment initiation, account information, payers and payees, and other payment service providers.[153]

On the other hand, coordination is often needed to mitigate retail risks in the payment services market. The proliferation of payment services provided by many entities has led to an increase in interoperability requests across many countries recently. As an example, interoperability has been a central element within the European Single Payments Area (SEPA),[154] a mission aimed at harmonizing retail payment markets across Europe. In order to prevent market segmentation, technical interoperability was created in SEPA through standardization (ISO 20022 - IBAN). At the national level, the requirement for interoperability could be further emphasized. The Central Bank of Jordan seeks to enhance confidence in the adoption of electronic payments and mitigate the risks associated with the split payment system. This gives the Central Bank of

[151] Committee on Payments and Market Infrastructure and the International Organization of Securities Commissions (2016) "Guidance on Cyber Resilience Khiaonarong and Goh Page 171 for Financial Market Infrastructures", Bank for International Settlements, available at: https://www. bis.org/publ/cpss101a.pdf (accessed May 18, 2023).
[152] Cyber Risk Adaptation Instructions issued by the Central Bank of Jordan in 2018.
[153] Newspaper Office of the European Union (2018) "Commission Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and the Council regarding regulatory technical standards for strong customer authentication and common and secure open communication standards.
[154] Ceiba. Short for "Single European Payments Area", it is an EU effort that seeks to provide a coherent and unified framework for electronic payments in euros across the EU and many European countries outside the EU. The goal of SEPA is to simplify and standardize international euro transactions, ensuring that they are as convenient, efficient and economical as domestic transactions.

Jordan formal authority to ensure the interoperability of payment solutions for the benefit of consumers and market growth.[155]

Hence, the Central Bank of Jordan has established a regulatory lab called BOX REG JO to facilitate the testing of fintech innovations. This lab provides entrepreneurs and developers with a controlled environment to evaluate digital financial applications using real customers. Its main objective is to promote and promote innovation and development in the field of financial technology while ensuring the promotion of financial technology. The aim is to enhance competition in the digital financial services sector, make commercial financial services more accessible, enhance usage tracking, and ensure the safety and stability of the financial sector while protecting the rights and data of your financial records. This document constitutes a regulatory framework that defines the working procedures of the Fintech Regulatory Lab at the Central Bank of Jordan. The lab is a critical component of the innovative and leading environment in the global financial sector. This framework is adjusted as necessary and whenever it deems appropriate to ensure the security of the financial industry. Furthermore, an individual is referred to as a banker. The Central Bank of Jordan ensures the protection and welfare of consumers. [156]

The researcher asserts that the Central Bank of Jordan has taken strides in introducing a legal framework to regulate the operations of electronic companies, traditional banks, electronic payment companies, and electronic transfer companies exclusively. However, there hasn't been a new addition to regulate electronic banking specifically; this is indeed what **the main hypothesis** of the research indicates and on which the research is based, which states the following: "Legislation has been implemented to limit identity theft and fraud in online banking. However, authorities are encountering challenges in establishing secure and authenticated digital identity procedures. New laws have been introduced to protect electronic bank customers, ensuring transparency in fees, conditions, and dispute resolution systems". The

[155] Central Bank of Jordan, Control and Control Department on the National Payment System, Sixth Annual Report, 2021.

[156] Box Reg Go The Central Bank of Jordan's FinTech and Innovation Regulatory Lab The Regulatory Lab focuses on innovative digital financial solutions in various financial activities, including saving, lending, insurance, and related digital services. It also covers electronic payment and money transfer, regulatory technology (RegTech) for risk management, fraud monitoring and reduction, digital services that provide access to finance and alternative financing, and digital services that support the digital transformation of the financial and banking sector.

Jordanian legislator must progress by establishing a dedicated legal regulation for electronic banks, encompassing electronic payments conducted digitally, distinct from conventional banking laws. This specialized legislation should cover all electronic operations and challenges, drawing from past experiences with international regulations. Drawing inspiration from examples like the European Union, where electronic banks such as Revolut Bank are licensed to operate, Jordan should consider implementing similar measures. This entails creating a separate legal framework tailored to the unique characteristics and requirements of electronic banking, ensuring it operates independently from traditional banking laws.

II.2. Responsibilities Of The Parties Involved In The Electronic Payment Agreement

The legal relationships between the parties involved in electronic payment systems are defined by their legal autonomy. Nevertheless, despite their autonomy, they are integrated within a cohesive legal structure. Consequently, the e-payment service provider and the e-consumer have reciprocal duties. The next section will address these pledges.

II.2.1. Responsibilities Of The Electronic Payment Service Provider

In accordance with Article (2) of the amended Central Bank of Jordan Law No. (24) From the provisions of Article (2016 laws), the National Preservation System is designed to provide electronic information services that facilitate the reception and processing of payment orders, transfer of funds wherever they are, clearing, settlement and payment services. Payment registration and turnover. A secure, efficient, internally financed system challenges the infrastructure of the financial and economic system and will facilitate the economy in the Jordanian market. It is also necessary to conduct transactions at the lowest possible cost, and this will also affect the growth and development of the national economy.[157] The electronic payment contract puts many obligations on the service provider, including the requirement for the electronic payment service provider to strictly comply to the comprehensive rules while delivering electronic payment solutions. The electronic payment service provider must adhere to the policies set by the Central Bank governing the processes and regulations for implementing

[157] National Strategy for Electronic Payments in Jordan The National Strategy for Electronic Payments in Jordan (2023-2025) issued by the Central Bank of Jordan.

electronic payment systems.[158] These policies vary from country to country, depending on prevailing financial and economic policies. They are crucial in protecting the general rights of users of the electronic payment system and in adhering to the principles that mitigate the risks associated with the provision of electronic payment methods, thus protecting users.[159]

The electronic payment service provider is eager to fulfill client demands and offer a wide range of electronic payment alternatives. The electronic payment service provider must accept client requests from the outset. The pledge is based on the authorization given by the Central Bank to offer electronic payment methods and streamline transactions inside the new electronic trading system. [160]

To ensure that e-consumers benefit from the services provided by e-payment service providers, service providers are responsible for providing the necessary means for this purpose. This includes providing the agreed payment method and making it available to the electronic consumer for use. Payment methods can be delivered physically, as in the case of bank cards and magnetic checks, or ethically, to other payment methods such as money transfer services and electronic money stored on computers or smartphones. In addition, the service provider must provide the electronic consumer with the required secret codes and software.[161]

The e-payment service provider has a responsibility to assist in the termination of the electronic payment system for the electronic consumer, and also to notify any instances of technical failures, theft, and loss. The electronic payment service provider must establish the requisite mechanisms to enable prompt termination of the electronic payment system by both the electronic consumer and the merchant in case of errors or circumstances necessitating its closure, such as incorrect secret access code entries or transfer order mistakes. On the other hand, the e-consumer may participate in fraudulent and misleading activities while utilizing this approach.

---

[158] Technical requirements for payment services companies and electronic money transfers issued by the Central Bank of Jordan 2018.

[159] Ibrahim, K. M. *Conclusion of the Electronic Contract - A Comparative Study*. Alexandria: Dar Al-Fikr Al-Jamia, 2006. p. 329.

[160] View the application form for licensing payment and electronic money transfer companies in the Hashemite Kingdom of Jordan issued by the Central Bank of Jordan in 2018

[161] Al-Aqabi, B. A., A. A. Al-Jubouri, and N. K. Jabr. "Electronic Money and Its Role in Fulfilling Contractual Obligations." *Ahl al-Bayt Magazine* 10, no. 6 (2008), p.125.

In fact, the electronic payment service provider is obligated to provide users of the electronic payment mechanism with reporting and notification mechanisms in case of theft or loss, and this is done to prevent unauthorized use by others[162], and the service provider is responsible for ensuring the safety and effectiveness of these devices and programs. The researcher believes that the responsibility of the electronic payment service provider is a pledge to achieve a specific result, as the mere assertion that it exercised reasonable care is not enough to absolve itself of responsibility for errors associated with electronic payment devices and software. Moreover, it is obliged to provide all the necessary electronic infrastructure requirements for electronic payment methods.

The obligation of the electronic payment service provider to maintain the privacy of customer data and transactions; electronic payment service providers are responsible for maintaining the confidentiality of customer information and maintaining it. This includes information from customers using the electronic payment service and merchants involved in electronic payment operations.[163] The service provider's obligation to this duty can be found in electronic payment contracts and may be imposed by legal provisions that require credit institutions to protect customer information and transactions. Any processing of this information must be carried out with the consent of the individual concerned, the electronic consumer.[164]

The e-payment service provider must maintain records and routinely deliver reports and data to the e-consumer. The electronic payment service provider is obligated to retain all documents pertaining to the transactions conducted by the electronic consumer. This includes preserving the records of the electronic payment methods offered to the consumer, their classifications and variations, the date of their provision to the consumer, and the transactions in which they were utilized. Determine the precise instances in which they were employed, including the relevant dates, times, and locations of purchase. [165]

Fulfilling electronic payment instructions is one of the primary responsibilities of the service provider. The main focus of the electronic payment contract is to ensure that the electronic payment service provider verifies the identity of the electronic consumer submitting the

[162] Ghannam, S. M. *Electronic Money Wallet*. Alexandria: New University House, 2007. p. 141.
[163] Tamimi, A. *Legal Regulation of Online Banking*. Alexandria: New University House, 2012. p. 429.
[164] Hijazi, A. F. B. *Online Consumer Protection*. Alexandria: Dar al-Fikr al-Jami', 2006. p. 52.
[165] Ibid, p. 55.

payment request, this is confirmed by the most important **hypotheses** on which the research was based, which state that" E-banks will face difficulties in complying with several financial rules, such as anti-money laundering (AML) and know-your-customer requirements, and the need to develop comprehensive strategies to manage their transaction scenarios.

in Jordan, the Know Your Customer (KYC) procedure is mostly based on paper documents and requires the personal presence of the customer. Conversely, KYC is a process that entails collecting data from identity papers, extracting digital information from government-issued smart ID cards, or using authorized digital IDs and facial recognition for verification.[166]

It is essential to verify that the order is placed by the authorized e-consumer as specified in the contract between them. The service provider can verify this using electronic signature, electronic customer password, or alternative authentication techniques. Furthermore, the service provider must guarantee that the money in the e-consumer's account are enough. Once the information has been verified and it has been confirmed that the e-consumer is the legitimate owner of the payment order, the service provider proceeds to carry out the request. [167].

In the same context, this is what I emphasized, the European Court of Justice (CJEU) ruled that contactless payment, or Near Field Communication (NFC), is a payment instrument under the EU Payment Services Directive 2015/2366 (PSD). The court clarified that banks cannot escape responsibility for unauthorized transactions by stating blocking NFC is impossible, consumer terms and conditions must adhere to Directive 93/13 on safeguarding consumer rights.[168]

Indeed, PSD2 is a critical regulatory framework that seeks to strike a balance between enhancing security for electronic payments, increasing competition in the payment services market, and improving consumer protection. Through the application. SCA[169] , creating opportunities for

[166] The Know Your Customer (KYC) process involves identifying and verifying the customer when establishing a business relationship and at regular intervals thereafter. Know Your Customer (KYC) regulations are under constant development and have gained global prominence across all industries. Due to the widespread spread of corruption, terrorist financing, and money laundering, the implementation of KYC regulations has emerged as a critical strategy in the global fight against financial crime. https://cutt.us/ApZ3l (accessed in 10 Step 2023)
[167] Ibid, p. 508.
[168] European Court of Justice (Case C-287/19 of November 11, 2020) Rules of Liability of Banks for Unauthorized Low-Value Transactions Using Contactless Payment, Library of Congress.
[169] Strong Customer Authentication (SCA); For authentication, SCA requires at least two of the following components; knowledge-based factors (such as password or PIN), possession-based factors (such as a mobile device or smart card), and rooted-based factors (such as biometric data such as fingerprints or facial recognition).

innovative payment solutions PSD2 aims to create a more secure and dynamic payment environment in the European Union. Payment service providers are required to comply with the provisions of PSD2 to ensure the security and transparency of electronic payment transactions within the European Union.

II.2.2 E-Consumer Responsibilities

The electronic payment service provides advantages to the electronic customer, but it also entails a set of obligations; the e-consumer must complete an application to join the electronic payment methods management system. The benefits of the electronic payment system are available to the e-consumer only upon seeking a contract from the electronic payment service provider. Upon joining, the customer must adhere to the terms of service, but the provider maintains the power to either approve or decline the consumer's request. The electronic payment service provider consistently examines the availability and compliance of the requirements for the electronic consumer who intends to utilize electronic payment methods for their account. If the e-consumer is a customer of the payment service provider, confirmation of compliance is typically instantaneous. Prominent folks might promptly utilize electronic payment methods.[170]

The consumer is obligated to furnish the payment service provider with the requisite information for the contract. The service applicant must supply the payment service provider with all the essential data to avail the service, which includes personal details like the applicant's name, address, and email, along with any additional information requested by the payment service provider. When giving this information, the online consumer must guarantee its precision and promptly inform the payment service provider of any circumstances that may necessitate changing this data. The consumer is fully accountable for any repercussions arising from an error in giving this information, as the service provider has the authority to discontinue the subscription. Providing inaccurate information by the e-consumer will result in their inability to utilize the payment system.[171]

The consumer's dedication to using electronic payment systems is efficient and convenient. One of the conditions stipulated in the contract between the electronic consumer and the

[170] Ibid, p. 509.
[171] Ibrahim, *Conclusion of the Contract by Electronic Settlement and Proof Thereof*. 2011. p. 262.

electronic payment service provider is that the electronic payment system must be used correctly, following the instructions provided and in the specified format. This proper use is necessary for the e-consumer to take full advantage of the system.

On the contrary, it is about the principle of acting in good faith when using the system, as outlined in the system's guidelines and the user guide provided to e-consumers who benefit from electronic payment methods. These instructions accurately outline the appropriate and optimal procedures for using the system, carefully reviewing all information provided to you by the bank or financial institution as it provides comprehensive information about the responsibilities you incur in exchange for obtaining the service or product. Before signing the contract, it is necessary to carefully research and understand the facts and responsibilities outlined, and confirm your ability to abide by them.[172] Furthermore, the e-consumer is prohibited from making any modifications that may affect the functionality of these devices, whether intentional or unintentional, it is necessary for the consumer to use these devices only in the intended way and refrain from using them in older devices. In addition, the user manual may include supplementary instructions. Failure to comply with these instructions is illegal use of electronic payment methods.[173]

Once the electronic payment service provider approves the consumer's request to join the electronic payment system, the customer is required to fully settle any payments made using the payment service supplied by the provider. The value of these fees is determined by the service provider. Irrespective of whether the service is utilized by the individual or by a third party, or if the electronic consumer authorizes others to use their payment methods, or if the service is accessed by others without their awareness, such as in instances of bank card theft or software hacking related to the payment service. Nevertheless, must persist in making payments to the service provider until he officially informs them of the occurrence of theft or hacking. The purpose of this is to guarantee that the service provider may promptly take necessary measures and notify shop owners who collaborate with them to refrain from taking payments through the compromised electronic payment method.[174]

[172] Instructions issued by the Central Bank of Jordan regarding the rights and responsibilities of the customer 2022.
[173] Ghannam, S. M. *Electronic Money Wallet*. Alexandria: New University House, 2007. p. 171.
[174] Ibrahim, *Conclusion of the contract by electronic settlement and proof thereof.* Previous reference. p. 266.

It is the responsibility of the electronic consumer to immediately report and report any cases of defect in the electronic payment method, theft or loss, and one of the primary responsibilities of electronic consumers is to immediately report any incidents involving malfunction, loss, theft or damage to the electronic payment system tools, as stipulated in the contractual agreements governing these mechanisms. In addition, e-consumers are obliged to inform the service provider if they suspect any errors in electronic payment processes or payment methods. [175]

This notification allows the payment service provider to meet its responsibility to the electronic consumer account and prevent any unauthorized usage. Therefore, it reduces the responsibility of the e-consumer for any transactions that take place after informing the service provider. In commercial contracts, the timeframe for this communication is typically specified using language such as "within a brief interval," "promptly," "without any delay," and "within the optimal timeframe." Nevertheless, there is a lack of agreement over the length of the notice period. Certain electronic payment contracts include the terminology "within a brief timeframe.".[176]

Restoring the electronic payment system's functioning is the consumer's obligation. The consumer's final responsibility is to restore the working tools and discontinue using the electronic payment system offered by the provider. This duty is in keeping with what was agreed upon in the customer-service provider agreement. Keep in mind that the service provider owns these tools and the consumer is only using them for a limited time. It is the responsibility of the e-consumer to respond when the service provider requests that the e-contractual consumer's relationship with the provider be ended, whether by expiration, termination, account closure, or any other means.

In addition, if the e-consumer requests to withdraw from the electronic payment system, he must return any associated tools in a functional, undamaged and usable state. However, it should

[175] Visa and MasterCard laws encompass chargebacks for fraudulent payments, non-delivery, and non-conformities. These limitations do not ensure that customers will have immediate access to chargebacks and are legally enforceable solely between banks. The facilitation of chargebacks is subject to the particular regulations set by card issuers in different Member States, which are regulated by the legislation issued by the card organization. The ECC Network receives funding from both the European Commission's Directorate General for Health and Consumers and Member States. The formatting and writing of this report have been carried out by the ECC offices listed below. ECC Norway is an organization based in Norway. The organization in question is ECC Czech Republic. The organization is known as ECC Germany. ECC Sweden is an organization.

[176] Boukhalfa, Hadda. *Electronic Payment Contract*. Oum El Bouaghi University, Algeria, 2022. p. 310.

be clarified that the products are not always in their original condition when they were first received by the e-consumer. Instead, they are in a satisfactory and legitimate state. Returning to these electronic tools is critical to prevent unauthorized users from accessing them and deter their illegal use in an attempt to breach electronic payment systems, in particular by internationally coordinated criminal organizations and Internet users[177]. Instead, it explains the type of payment that the e-consumer makes to the bank when acquiring this tool. This payment allows the consumer to benefit from the tool by using it for payment transactions, but ownership of the tool remains with the payment service provider. The service provider has the right to terminate the payment method or withdraw it from the electronic consumer without notice or explanation.[178]

In fact, PSD2 is an important regulatory framework for the European Union designed to modernize and secure electronic payment services. Here are more specific details, examples and procedures related to PSD2: Strong customer authentication (SCA); [179]It is the cornerstone of PSD2 and aims to enhance the security of electronic payment transactions. It requires two or more authentication factors, for example; When making an online payment, the consumer may be asked to provide something they know (e.g., a password), and something they have (e.g., a one-time code sent to their mobile devices), and something that they know (for example, fingerprint) from where the law exists, the European Union sets the Regulatory Technical Standards (RTS) for the SCA in the Delegated Regulation (EU) 2018/389.

[177] Instructions issued by the Central Bank of Jordan regarding the rights and responsibilities of the customer 2022.
[178] Tamimi, *Legal regulation of online banking.* p. 510.
[179] SCA. Short for "Strong Customer Authentication", it is a security feature used in electronic payments and online banking to enhance the protection of user accounts and transactions. Strong Customer Authentication (SCA) is required under regulatory frameworks such as the European Union (EU) Revised Payment Services Directive (PSD2). Its purpose is to reduce the potential for fraud and enhance the security of electronic payment transactions.

Third-party payment service providers (TPPs)[180] are those that include payment initiation service providers (PISPs) [181]and account information service providers (AISPs).[182] These entities can access customer account information and initiate payments with the customer's consent. For example, a consumer can use TPP to aggregate financial data from multiple accounts in a single app or to initiate payment directly from their bank account. In terms of law, the Revised (PSD2) provides the same relevant laws and laws. Legal framework for the Trans-Pacific Business Partnership.

On the other hand, account access (XS2A) requires banks to provide TPP certified partners with access to customer accounts to foster competition and innovation in the financial sector. For example, when a consumer uses a third-party app to view their bank account balance or initiate a payment, this includes XS2A[183]. PSD2 touched on a very important issue, which is consumer consent. Consumers must explicitly give consent to TPP partners to access their financial data or initiate payments on their behalf. Example: Before the TPP can access customer account information, the customer must provide consent. Through their banking platform or TPP, and in terms of law, the provisions regarding consent are detailed in PSD2 and associated regulatory guidelines.

In terms of complaint handling and liability, PSD2 sets out dispute resolution rules and assigns liability in cases of unauthorized or fraudulent transactions, providing protection for consumers.

---

[180] TPP "Third Party Provider" is what it stands for. In the context of financial services and regulations like the updated Payment Services Directive (PSD2) in the EU, TPPs are businesses that cater to both people and institutions with a variety of services. One of these services is the ability to see a customer's financial records and even make a payment for them. These services aim to boost innovation and competition in the financial industry; they are generally built on top of open banking.

[181] PISPs, short for payment initiation service providers, are regulated financial institutions or third-party providers that provide payment initiation services in the context of open banking and finance. PISPs operate within the legal framework set out in the revised Payment Services Directive (PSD2) in the European Union (EU) and similar rules in different countries.

[182] AISPs, also known as account information service providers, are a specific category of third-party providers (TPPs) in the financial services industry. It is regulated by the revised Payment Services Directive (PSD2) in the European Union. AISPs offer services focused on retrieving and consolidating user financial data from many bank accounts, offering analytics and information related to these accounts, and AISPs are essential in the open banking ecosystem because they provide users with a more comprehensive and easier way to oversee their finances. Individuals can leverage the services of Account Information Service Providers (AISPs) to monitor their financial activities across multiple banks, develop custom budget plans, and gain valuable knowledge about their spending habits. This facilitates the disclosure of financial information and enables consumers to make informed financial choices.

[183] XS2A, short for "Account Access", is a core concept in the field of open banking and finance in the European Union (EU). XS2A is a core concept defined in the revised Payment Services Directive (PSD2), a legislative framework designed to promote competition, innovation and security in the European payments sector.

In case of unauthorized payment, PSD2 establishes a clear process for consumers to dispute the transaction and request a refund and defines PSD2's liability and dispute resolution mechanisms and related guidelines. Together, these provisions and their associated laws form the legal framework of PSD2, ensuring that electronic payment systems within the EU are secure, competitive and focused on consumer protection. The researcher agrees that it is comprehensive and covers all financial transactions related to electronic banks, and payment service providers must adhere to these controls to protect consumers and maintain the integrity of electronic payment transactions; This is what the second part of **the first sub-question** actually indicates, which states, to what extent are the legislative developments accelerating for electronic banks in light of international regulatory developments and the European Union? From the above, it is proven to us the extent of advanced regulatory legislation in the field of electronic banks in the EU.

As a result, People are worried about their privacy when personal information and financial transactions are gathered, stored, and used. When looking at the dangers of online payments, it's obvious that regulatory approaches and their underlying laws should fortify entity-based regulation, with an increased emphasis on actions, in order to safeguard personal information and privacy rights, as is the case with regulations like the EU's General Data Protection Regulation (GDPR). In the past, payment networks and other similar organizations were the primary targets of financial regulators' efforts to keep an eye on the industry as a whole. For various types of providers, including well-known fintech and huge tech businesses, to be able to fit into the correct regulatory framework, licencing processes must be reshaped. Payment services may be efficiently regulated by authorities using a systematic manner. Find out if the primary business function can be described as a payment service. Concerns regarding safeguarding monies, preserving financial integrity, guaranteeing cybersecurity and data security, and easing access to payment systems and interoperability are examples of new hazards that the present regulatory framework may not have sufficiently addressed. The provision of payment services requires an open, thorough, and strong legal framework, which can only be achieved by increasing legal certainty. The emergence of payments and developments in fintech have raised worries and regulatory difficulties for central banks. With their growing influence on payment stability, financial stability, and the transmission of monetary policy, monitoring payment activities is crucial. Compliance with international standards and other regulatory

requirements is required due to the developing nature of payment operations and the increased possibility of systemic risk.

Indeed, Jordan has the Cybercrime Law of 2015, which serves as the empowered legislation addressing risks stemming from electronic operations in general. However, there remains a notable absence of independent and comprehensive legislation specifically tailored for electronic banks and all their operations. It's worth noting that many countries around the world are still in need of enacting legislation for the protection of electronic operations and transactions. Therefore, there is a pressing need for Jordan to develop dedicated laws and regulations that cater to the unique challenges and requirements of electronic banking to ensure the security and integrity of electronic transactions in the digital age.

Banks' electronic services are distinguished by their rapidity, adaptability, and straightforwardness. Hence, the presence of distinct, autonomous, and swiftly evolving legal regulations is vital to safeguard and foster confidence among consumers in electronic banks and electronic payment transactions, which have experienced substantial growth during and post the COVID-19 epidemic.

Indeed, customers are accustomed to having recourse to references when encountering problems or submitting requests, as is the case with traditional banks, where customers can seek assistance during working hours to resolve any issues they may face. Therefore, there is a pressing need for central banks to intervene more comprehensively and accurately in order to delve into the intricacies of electronic financial operations. This intervention is essential to develop a robust legal and legislative framework for electronic financial regulation that instills confidence in customers and compels electronic banks to adhere to the legal foundations established by the Central Bank, thereby safeguarding the interests of all parties involved. This legislation must evolve in tandem with the advancements in financial technology and the accelerating challenges it presents. By staying abreast of these developments and continually refining the regulatory framework, central banks can ensure the security, integrity, and trustworthiness of electronic financial operations, thus fostering a conducive environment for the growth and sustainability of electronic banking services.

The researcher believes that The Central Bank of Jordan has implemented measures to establish a legislative regulatory framework only for electronic corporations, traditional banks, electronic

payment companies, and electronic transfer companies. The Central Bank of Jordan has formulated a comprehensive definition of the term "company" which encompasses both public and joint stock companies. These are private firms that have been granted permission to provide electronic payment services and oversee the operation of electronic payment systems. This term does not have legal implications for independent electronic banks, as they electronically handle and control the same systems that are operated behind screens. The Jordanian lawmaker should develop a specialized system for electronic banking, which would include electronic payment operations and other related activity undertaken online. The lawmaker must urgently enact a separate and unique legislation for electronic banks, apart from the restrictions that apply to traditional banks. This specific legislation should thoroughly regulate electronic payment operations and all other electronic transactions, including the associated obstacles. By implementing this approach, the legislator may establish a comprehensive set of rules and regulations that effectively protect the interests of all parties participating in electronic banking services in Jordan. This will ensure that electronic financial transactions are secure, trustworthy, and dependable.

In fact, Jordan's regulatory framework needs to strengthen the focus on financial consumer protection, competition, innovation, and standardization related to the provision of payment services, such as the pricing policy of payment services in the realm of fairness and transparency. Deficiencies in some standards of full integration and interoperability in Jordanian laws, leading to inappropriate user experiences. In addition to the insufficient levels of awareness and financial literacy among financial consumers regarding electronic payments, low rates of access to electronic payment services, limited reliance on electronic payments, and limited innovation in the fields of electronic payment. Carrying out substandard business operations. As a result, consumers continue to rely on cash and checks, as is well known, and the relatively high cost of payments in the Jordanian economy, as well as low levels of financial inclusion rates in receiving electronic payment services.

This leads to confirming the first part of one of the **important hypotheses** in this research, International coordination and cooperation between regulators is needed for the proper international management of electronic banks, which may lead to a combination of legislative regulations; and different jurisdictions to adapt and define appropriate jurisdiction and criteria

for disputes involving e-banks, So that the legislator can put in place the legal organization to confront the regulatory challenges that cause an obstacle to opening the door to investing in full electronic banks in Jordan. The European experience is also an advanced experience in this field, and many electronic banks have been established in Europe and have succeeded, especially during the Corona pandemic. Therefore, the researcher recommends taking the European experience as a primary reference for the Jordanian legislator and decision-maker to put in place a framework for organizing a banking financial law that keeps pace with the latest advanced legislation.

Hence, it is essential for the Jordanian legislature to address the following matters: Formulating policies and protocols geared towards diminishing reliance on traditional and cash-based payment methods while bolstering the adoption of electronic payments. Identifying suitable strategies to nurture and promote innovation within the electronic payment sector, alongside implementing effective measures to lower transaction costs across the economy. Additionally, raising awareness levels and enhancing financial literacy, as well as augmenting financial inclusion rates in Jordan, are imperative objectives.

II.3. Criminal Protection Of Electronic Banking Operations In Jordan

The advancement of information technology has significantly transformed the banking sector, enabling banking activities to be conducted online. This shift has given rise to new electronic services offered by banks, necessitating electronic means for their execution. However, this technological progress has also made the banking sector susceptible to cyberattacks. In response, legislators have taken measures to criminalize such acts. This analytical section aims to examine the provisions pertaining to the criminal protection of electronic banking operations outlined in the Cybercrime Law. Its objective is to assess whether these provisions are adequate in providing protection against cyber threats.

Electronic banking services, which replace traditional paper-based methods with electronic platforms such as web and mobile applications, are accompanied by significant security risks stemming from cybercriminals and fraudsters who exploit financial information. To combat these threats effectively, a robust security system must be in place, which includes data encryption and multiple authentication procedures. In 2020, the significance of digital financial services and e-commerce greatly increased as a result of the COVID-19 epidemic, which led to

millions of people spending more time at home. Nevertheless, the growing dependence on digital platforms has led to a significant surge in cybercriminals' utilization of social engineering methods to exploit victims. Hence, it is imperative for both financial institutions and clients to maintain a high level of vigilance and awareness regarding prevalent fraudulent strategies and schemes, in order to properly safeguard themselves.[184]

The increasing reliance—and maybe even the overreliance—on technology in carrying out financial and banking activities is a major contributor to the increasing complexity of compliance work inside these organizations. More and more financial activities are being outsourced to artificial intelligence (AI) systems, and there has been an uptick in interaction with fintech organizations, all of which contribute to this reliance on fintech. Minimizing human interaction in banking processes is the main objective of this movement. Its purpose is to save expenses and expedite transaction processing. The dangers that come with our increasing dependence on technology and automation, meanwhile, go well beyond the domain of the web and IT. Among these dangers might be malfunctions in operations, theft of personal information, or holes in artificial intelligence systems. As a result, the task of keeping up with the ever-changing regulatory landscape while also ensuring effective risk management and regulatory compliance falls on the compliance divisions of banks and other financial institutions.

Information technology has facilitated the means of life, and in turn has facilitated the means of committing crimes. Therefore, new terms have emerged in criminal science, such as cybercrime, cybercriminal, cyber victim, and evidence. It is very natural that the negative side of information technology is exploited and used as a means to commit crimes that are difficult for some crimes to occur, or that crimes occur because of this technology, and new types of crimes appear as a result effectively out of respect for adapting them according to traditional penal texts, which in most cases are unable to face these problems due to the principle of legality; many legislators have realized this and enacted Legislation in various ways criminalizing forms of assault.[185]

---

[184] Garmon, David. *Information Security Policy Preparation Guide*. GSEC Air Navigation Services Security Fundamentals Practical Mission, version 1.3. SANS Institute, 2002. p. 19.
[185] Laxana, Rio Danny, Intan Shafiri, and Humira Nazini. "The Impact of Operational Risk on Electronic banking in Banks." *Journal Management Business* 14, no. 2 (2023). p. 459.

Information technology has become increasingly intertwined with criminal activities, and electronic banking operations have not been immune to this trend. Recognizing the pivotal role of electronic banking in the economy, legislatures have included provisions for criminal protection within banking laws. Banking operations are vital pillars of any country's economy and are instrumental in driving growth and development across various social sectors. The advent of the Internet has revolutionized economic activities, giving rise to phenomena such as e-shopping, electronic money, and digital documents. E-commerce has fundamentally altered investment practices and banking procedures. Given the significant role that banks play in our lives, they are now prioritizing the enhancement of their financial services to gain a competitive edge. This is achieved through electronic banking operations, which enable customers to access a wide range of banking services via the Internet. These services include depositing funds, making payments, transferring money, and more, all accessible anytime and from anywhere.

Electronic banking services offer numerous advantages, providing customers with convenience, efficiency, and time savings at a reduced cost. Banks prioritize ensuring that electronic banking is accompanied by robust cybersecurity measures, data protection protocols, and safeguards for customer privacy. Despite these efforts, electronic banking operations are susceptible to technical risks, including attacks such as data hijacking, fraud, and forgery of documents and electronic cards. To address these concerns, modern legislation places a strong emphasis on providing criminal protection for electronic banking operations. In Jordan, the legislator has allocated Articles 6 and 7 of the Cybercrime Law to address crimes committed against electronic banking operations. Article 6 criminalizes the unauthorized acquisition of data or information related to credit cards, as well as data or information used in conducting financial or electronic banking transactions. Article 7 criminalizes attacks on electronic banking services, further reinforcing the legal framework for protecting electronic banking operations in the country.

To safeguard themselves and their customers from constantly evolving fraud tactics, online banks must implement measures such as reducing the number of login attempts required to complete a transaction (cybercriminals may try multiple times before finally succeeding), educating customers about the tactics used by online criminals, and regularly supplying them with information on how to recognize fraud and what to do in such situations. Perform evaluations The establishment of a dedicated fraud analysis team that can spot new techniques,

the adoption of multi-factor authentication to make it harder to get access to accounts, and the execution of regular security and penetration tests to identify any weaknesses in the company's network are all steps taken to ensure the safety of data, systems, and applications [186].

II.3.1. Criminal Protection Of Credit Card Data And Information

Article (6) of Jordan's Cybercrime Law stipulate: "Anyone who deliberately obtains credit card data or information through the information network or any information system shall be punished..." Before we discuss the material and moral elements of this crime, we will clarify the subject of the crime, which is data or information related to credit cards.

II.3.1.1. Crime Scene

The subject of this crime is data or information related to credit cards. Jordan's cybercrime law defines data as "numbers, letters, symbols, shapes, sounds, images, or graphics that have no meaning in themselves." It also defines information as: "data that has been processed and has become important" Data is the raw material of information. This is because pre-processing data has no meaning per se, and therefore the legislator has included data and information in protection, which is commendable and would expand protection.

However, the data and information protected in this crime must relate to credit cards. Knowing what the merchant is meant by credit cards requires identifying and distinguishing them from other bank cards and evaluating the plan of the Jordanian legislator.

II.3.1.2. Evaluation Of The Jordanian Legislator's Plan

Article 6 of the Cybercrime Law criminalizes the acquisition of data or information related to electronic banking transactions. However, there is a desire among some stakeholders for the legislator to broaden the scope of this provision to include all types of electronic cards, not just credit cards. This is because electronic cards encompass a variety of types, including loyalty cards, ATM cards, and cheque guarantee cards, each with its own unique identity and functions. Those familiar with comparative Arab legislation may note that criminalization in other jurisdictions is not limited to obtaining data related to credit cards but extends to all types of

[186] Hamidi, N. A., Mehdi Rahimi, J. K. Navarya, and B. Robertson. "*Personal Security Approaches in Electronic Banking Using Flask Architecture on the Cloud*." 2013. p. 24.

electronic cards. Therefore, there is a call for the Jordanian legislator to consider expanding the scope of Article 6 to cover all electronic cards, ensuring comprehensive legal protection against unauthorized acquisition of data or information related to electronic banking transactions.

For the purpose of exploration and taking a look at some Arab and international legislation in this regard article (11) of the UAE Information Technology Crimes Law criminalizes the use of the information network or information technology means to access it without the right to obtain credit card numbers, data or other electronic cards, and Article (28) of the Omani law criminalizes infringement of financial cards, so that protection extends to all cards.[187]

Since the assault on these cards does not depend on mere access to data and information related to them, some legislations have criminalized the forgery of these cards, such as the Omani legislation[188] , and the Syrian law criminalizes the forgery of payment cards[189] and the use of counterfeit, stolen or lost cards to pay or withdraw money. [190]

Article (12) of Qatari law criminalizes obtaining electronic transaction card data and numbers, forging a counterfeit card, using forged cards, or knowingly accepting a stolen card. Article 148 of the Swiss Penal Code criminalizes the legal holder's use of a cheque guarantee card, credit card or any similar means of services that the card can provide, in order to harm the investigation of any party. Card grantor, according to for the contractual terms concluded between them. In Finland, Chapter (17), Article (8) of the Act punishes, in addition to penalties, "anyone who seeks financial gains without any right for himself or a third party, by using a bank card for payment, credit or any other means. Other similar payments without permission or by exceeding the legal permission of the cardholder or using the card by the cardholder to withdraw more than the balance or beyond the maximum allowable limit".[191]

---

[187] Unauthorized access to information networks or technological methods is usually criminalized under Article 11 of the UAE's Information Technology Crimes Law. Any person using information technology without permission or obtaining unauthorized access to the information network will be punished in accordance with this clause. In contrast, Omani legislation (Article 28) punishes bank card fraud and protects cardholders from fraud and manipulation fees. In contrast to Omani law, which focuses directly on the misuse of financial cards, UAE law addresses a wide range of illegal access.

[188] See Article (2) of the Cybercrimes Law No. 27 of 2015 in Jordan.

[189] Ridwan, F. N. *Credit Cards*. Al-Jalaa Al-Jadida Library, 1990. p. 17.

[190] Al-Hamoud, F. *The Legal System of the Credit Card*. Dar Al Thaqafa Publishing and Distribution, Amman, 1999.p.15.

[191] Salem, M. *The Criminal Protection of the Loyalty Card*. Dar Al Nahda Al Arabiya, 1st edition, 1995. p. 1.

The discussion above highlights the deficiencies in Article (6) of the Jordanian Cybercrime Law. These shortcomings include the insufficient protection provided for all types of electronic bank cards and the absence of provisions criminalizing forgery, theft, and the legitimate use of a bank card by its holder. Adapting these acts to traditional legal provisions presents challenges.

Anyone found guilty of assaulting banking operations as described in Articles (3 to 6) of the Cybercrime Law faces severe penalties, including temporary hard labor for a minimum of five years, along with a fine ranging from 5,000 to 15,000 dinars. This categorizes the crime as a felony. Regarding attempted acts, the penalty depends on the specific offense committed. While the crimes outlined in Articles 3 to 6 are initially considered misdemeanors, attempting to commit these acts involving electronic banking operations elevates them to felony offenses. In cases where the attempted act does not result in the intended outcome, the offender is subject to punishment under the Penal Code, as the Cybercrime Law lacks specific provisions for attempts.

In Articles (21 & 22) of the Jordanian Electronic Transactions Law, the Jordanian legislator focused on establishing the prerequisites for licensing electronic transfer and payment companies, as well as outlining the procedures for operating the electronic payment system. However, these provisions lacked elaboration on other aspects. Despite having advanced infrastructure in digitization, Jordan faced challenges in service delivery, leading to delays that affected citizens; The above indicates and confirms that This is what is actually raised as a **second sub-question in this research**, and it deals with The second sub-question: What weaknesses does the Jordanian Electronic Transactions Law include in light of the international model and directives of the European Union".

On a positive note, the Ministry of Digital Economy and Entrepreneurship in Jordan successfully implemented 450 automated services, widely utilized by citizens. Furthermore, there is a growing trend towards consolidating information services accessible through the national citizen number, encompassing social security, property, national assistance, and various documents, streamlining accessibility for citizens.[192]

The Jordanian digital identity is poised to become a primary alternative to traditional forms of identification in the future. It will encompass all pertinent information from various databases

[192] Introduction from, Ministry of Digital Economy and Entrepreneurship in Jordan. (2021).

relevant to citizens, streamlining service delivery processes with enhanced efficiency and reduced costs. The National Strategic Plan for Digital Transformation, along with its Executive Plan up to 2025, has been formulated in alignment with national policies, strategies, and global digital transformation trends. The plan encompasses infrastructure development and its various components, data management, and the enactment of pertinent legislation, notably the Personal Data Protection Law. This legislation safeguards individuals' data, prohibiting its unauthorized use by any entity without the owner's consent. Moreover, the plan emphasizes the digitization of services and collaboration with the private sector to achieve these objectives effectively.

The establishment of a technologically-based infrastructure is essential for the laying of the groundwork for electronic banking and, more broadly, electronic commerce. Not only do contemporary forms of communication and information meet the necessary legal and regulatory standards, but they also fit in with the cultural and social context of online transactions [193] .

II.3.1.3. Physical Element

The material element of the crime of obtaining data or information related to credit cards is defined by the legislator in Article 6 of the Cybercrime Law. The law states that "everyone who obtains it" commits the offense. This indicates that the criminal activity involves any action that results in gaining control over data and information related to credit cards. The offense is characterized by positive behavior, as the offender actively seeks to obtain the data and information. Negative behavior, such as refraining from obtaining the data, does not constitute the crime. Additionally, the acquisition of data must occur through an information network or any information system to qualify as a criminal offense. An information system is described as a collection of programs and tools designed for creating, transmitting, receiving, processing, storing, or managing electronic data or information. Meanwhile, an information network links multiple information systems to facilitate data exchange and retrieval. Unauthorized access to such networks or systems, without the permission of rightful owners, is considered a criminal offense. Although the law does not explicitly require illegal access to an information network or system for obtaining credit card data, the offense is committed in such scenarios.

[193] Ghanam, S. M. *The Responsibility of the Bank for Computer Errors in Electronic Funds Transfer*. Cairo: University Publishing House, 2010. p. 13.

Additionally, the crime can occur even with legitimate access if the data and information are obtained without authorization. In essence, the law covers both situations, emphasizing that the crime is only committed when the perpetrator successfully obtains the data and information. Attempting to obtain such data without success does not constitute a crime. Therefore, this offense is categorized as one with full consequences, meaning it is only considered complete upon achieving the desired outcome. If unauthorized access is made to an information network or system without obtaining credit card data, it falls under the offense of unauthorized access as stipulated in Article (3/a) of the Cybercrime Law.

II.3.1.4. Ethical Pillar

The crime of obtaining data and information related to credit cards is considered a deliberate crime, and the legislator expressed this by saying in Article (6) "Anyone who deliberately obtains ... punishable." The offender must know the truth of his behavior and the elements of the result, if a person initiates a behavior that results in the realization of the act and his intention to crime, and if he wants to suffer this result, he will not be held accountable for this crime, because it is not committed and the information related to credit cards is not transmitted by mistake.

It remains to be said that the intent required in this crime is a general criminal intent, and it does not matter the motive for committing the crime afterwards, although in most cases it is with the aim of obtaining material benefits by obtaining data and information related to the card[194].

[194] In 1995, the term "phishing" emerged, referring to attempts to obtain personal or financial information from internet users through emails or websites. Fraudsters send fake emails asking users to visit a website to update their information, such as username, credit card password, social security number, or bank account number. These websites are fake, designed solely to steal user information. Users enter their email and password, not realizing the need to review these entries, allowing organized crime groups access to electronic payment card numbers. These groups have access to the "shadow of the crew."
For example, in 2007, Thai authorities arrested three Sri Lankan men and confiscated 5,000 fake credit cards bearing the names of British individuals. It was discovered that these men had used the cards multiple times to withdraw money from ATMs. One method of electronic fraud is conducting deceptive online auctions and mediating in various fields by inflating and deflating the price of sold items to raise the stock value of an economic institution, such as a company, in the financial market. For more details, see Grabusk B.: The Internet and Technology.

II.3.1.5. Punishment

The individual who commits the offense of unlawfully acquiring credit card data and information will be subject to imprisonment for a minimum of one year and a maximum of three years, as well as a fine ranging from 500 dinars to 2000 dinars [195].

Criminal protection of data and information of financial and electronic banking transactions. In Article (6) of the Cybercrime Law, the legislator criminalizes obtaining without a license through the information network or any data or information related to credit cards, data or information used in conducting financial or electronic banking transactions. The first part of the criminalization concerns credit cards, while the second part concerns electronic financial and banking transactions. This crime does not differ from the previous one in material and moral aspects, as well as the punishment imposed on the perpetrator. For repetition, we will point out that the difference lies only in the place where the crime occurs. In order to prevent the elements of this crime, we refer to the elements of the crime of obtaining without authorization data or information related to credit cards.

The subject of this offence is the data and information used in conducting financial or electronic banking transactions. Therefore, it is necessary to know the financial or electronic banking transactions, and explain the banking and financial operations, including the concept of financial transactions in their natural form, and the banks and financial institutions that carry out banking operations, and then electronic banking.

II.3.2. Criminal Protection Of Financial And Banking Operations

The Jordanian commercial law addresses the regulations pertaining to current accounts in Articles (106 to 114) . These articles outline the terms governing cash deposit contracts, along with Article (116) concerning deposit contracts. Additionally, Article (117 & 115) elaborate on

[195] appears to suffer from poor wording regarding the limits of imprisonment, which is one of the penalties prescribed for misdemeanors. The duration of imprisonment for a misdemeanor in Jordanian legislation ranges from one week to three years unless the law states otherwise (Article 21 of the Penal Code). For those who read the text of the general provisions, without knowing the limits of the penalty for a misdemeanor in Jordanian legislation, the maximum penalty of imprisonment is three years. The drafters of the text could have sufficed by stating the minimum penalty for imprisonment, and therefore the maximum penalty for imprisonment would be (21) of the Penal Code.

related aspects. Furthermore, ordinary articles (118 to 121) delineate provisions regarding leasing arrangements, including lease contracts for iron safes, and other relevant documents. Given the intricate, varied, and constantly evolving nature of banking operations, it is challenging to provide an exclusive definition of such operations.[196] There is a population that increases or decreases in banking activities, and it is a society that develops with the development of circumstances and the difference in time and place because banking began as simple and expanded like most commercial activities [197].

Banking operations encompass three primary categories: bank accounts, deposits, and credit operations. Bank accounts consist of current accounts and bank transfers, while deposits include cash deposits, securities deposits, and deposits in iron safes. Credit operations comprise financial credit, documentary credit, letters of guarantee, and discounts on commercial papers. According to Article (2) of Jordanian banking law No. (28) of 2000, banking operations are defined as the acceptance of deposits from the public through the central bank, and utilizing these deposits, either wholly or partially, to extend credit or engage in other financial activities. This definition underscores the significance of credit operations within banking activities. Moreover, banks offer various additional services beyond deposit-taking and lending, such as check deposits, collection of commercial and financial paper proceeds, safe deposit box rentals, customer rights management, payment facilitation, and investment services using customers' funds. As for Act No. (11) of 1969, the Jordanian legislator regulates the provisions of certain banking operations in the Commercial Code in articles (106 to 122), as for banking operations not mentioned in these articles, article (122) of the Commercial Code refers to the provisions of the Civil Code, which stipulates that "banking operations not mentioned in this chapter are subject to the provisions of the Civil Code relating to the various contracts resulting from the said operations or the contracts that characterize such operations".

Article (7) of the Cybercrime Law stipulates that: "Whoever commits one of the acts stipulated in paragraphs (3), (4), (5) and (6) of this law shall be punished if he signs an information system, website or information network." Banking services related to the transfer of funds or the provision of payment, clearing or settlement services provided by banks and financial

[196] Reda, El-Sayed. *The Banking System and Banking Operations*. 2000. p. 121.
[197] Ali, Gamal Eldin Awad. *Bank Operations from a Legal Perspective*. Dar Al Nahda Al Arabia, 1981. p. 2.

companies shall be subject to temporary hard labor for a period of not less than five years, and a fine of not less than for (5,000) five thousand dinars and not more than (15,000) fifteen thousand dinars." It will become clear to us through the explanation of the text of the previous article that it suffers from legislative deficiencies, and that it is difficult to separate some forms of this crime from the crime mentioned in Article (6) of the same law, which is the crime of obtaining information or data related to electronic banking operations, and the legislator had to increase the penalty,[198] as this is a crime if some circumstances exist, as some legislation does. I have no choice but to clarify the provisions of this article, despite its poor wording, clarifying in the first requirement the material element, and in the second requirement is the moral element, and in the third requirement the penalty. In one of the most prevalent scams, attackers commonly employ two tactics to access accounts, which are a continuation of similar trends observed in 2019. In the first tactic, fraudsters disguise themselves as "saviors" by claiming to be security experts. They fabricate scenarios to convince users that they are in imminent danger and offer to rescue them these criminals often contact bank customers, pretending to be responsible for digital security. They request fees or payments while pretending to offer aid and support. Rescuers may request clients to confirm their identification by providing a code through a text message or app notification. This is done to prevent unauthorized transactions or transfer of cash to a "secure account." Additionally, the rescuers may also urge their victims to install a remote management app, under the guise of needing assistance with issues. Scammers frequently impersonate staff of major banks in the area of their intended targets, and apply a deceptive phone ID to make it appear as if the call originated from an actual bank number.

II.3.2.1. Material Element

The legislator has outlined the crimes specified in articles (3 to 6) of the Cybercrime Law, necessitating an explanation of both the criminal behavior and its consequences. The criminal behavior associated with attacking electronic banking operations manifests in various forms. Firstly, it involves intentionally accessing an information network, system, or website without proper authorization or in violation of the law. If this unauthorized access pertains to networks,

[198] Article 7, Jordanian Cybercrime Law.

systems, or websites linked to banking services provided by banks or authorized financial institutions, the perpetrator commits the offense of unauthorized access. [199] However, what distinguishes this crime is the specific location of the unauthorized entry, which must be related to the provision of banking services. The legislator has specified the forms of banking services, such as payment services, clearing, or settlement, and has subsequently issued provisions for each type of service. Despite having elucidated the forms of electronic banking operations, the concept itself remains ambiguous. Thus, there is a need to provide clarity on the broader understanding of electronic banking operations; This is indeed what **the main hypothesis** of the research indicates and on which the research is based, which states the following "Legislation has been implemented to limit identity theft and fraud in online banking. However, authorities are encountering challenges in establishing secure and authenticated digital identity procedures. New laws have been introduced to protect electronic bank customers, ensuring transparency in fees, conditions, and dispute resolution systems.".

Credits and debts are transferred electronically from one bank account to another bank account[200], and the legislator has increased the penalty in the event of unauthorized access if the online store is linked to electronic services, although it punished deliberately obtaining without permission through the information network or any information system data or information related to electronic banking operations. Here the contradiction appears, as the scope of Article (2) of the Cybercrime Law criminalizes access in a broader sense than just entry. It is logical to expect that mere access to an online platform containing sensitive data regarding banking transactions would incur a more severe penalty compared to simply obtaining such data. Conversely, engaging in activities involving intentional access, publication, or utilization of information related to banking services provided by financial institutions through an information system, website, or information network warrants significant legal consequences. Such actions may include manipulating, altering, or tampering with data or information, as well as disrupting or disabling the operation of an information network, system, or website. Perpetrators may employ tactics like introducing malicious programs such as viruses to accomplish these

[199] Nilofer, S., Ridwan, W., and Peter, G. "Unauthorized Access to the Wireless Local Area Network: Two Constraints Imposed by Current Australian Laws." *Computer Law and Security Net Review* (2009), p.25, & Kim, C., Neuberger, B., and Shack, B. "Computer Crimes." *Computer Crime* 49, no. 2 (Spring 2012), p.9.

[200] Survey; it is the retention of a debt owed to a creditor by a debt owed from him to his debtor (Article (343) of the Civil Code). For information regarding electronic set-off, see Hazem Al-Samadi: Responsibility in Electronic Banking Operations, Dar Wael, 1st Edition, 2003, p. 32 and following.

objectives [201], and other malware through the information network or information system If the software is distributed in any way through the information network or information system. Article (2)of the cybercrime law defines a program as a set of technical commands and instructions designed to accomplish an actionable task using information systems.

The intent of the actor when presenting or publishing programs is crucial, particularly when the aim is cancellation, which entails the removal of data or content either entirely or partially. In essence, deletion carries the same connotation as cancellation, though the latter is often considered a more technical term. Both terms signify the act of removal. Conversely, addition refers to the act of increasing or adding content or data. Whatever the type or form of destruction, it takes the form of complete destruction of the thing, and detection is achieved by publishing and broadcasting, while destruction leads to damage to the thing, and concealment results in concealment, prevention and concealment[202].

Secondly, the amendment involves altering the system or information data, whether it necessitates specific changes such as additions, deletions, or replacements. The action carried out by the perpetrator in the event of modification is deliberate and aims to achieve a particular outcome. This result is predetermined either in the mind of the offender or may be envisioned as achievable by the offender.[203]

The change has a broader and more comprehensive concept, as it can be in the form of adding, modifying or deleting, and the transfer leads to a change of location. Copying occurs in the case when data and information are obtained and their content is transferred without this resulting in the loss of the original from which it was copied. Suspension occurs in case of prevention and obstruction from work, and disruption means sabotage, whatever its form or extent.

Third, capture, interception, obstruction, change or deletion of data or information transmitted through the computer network for electronic banking services provided by banks or financial companies. Interception is the process of intercepting messages sent by electronic means by

[201] The input is considered a form of the material element of the crime of disrupting the system's work according to Article Two of the UAE Cybercrime Law, Article Four of the European Convention on Cybercrime, and Article Two of the Arab Model Law.
[202] Article 3/323 of the French Penal Code criminalizes the act of maliciously entering data into a data processing system, or maliciously deleting or modifying such data. Anyone who commits this act is punishable by imprisonment for up to three years and a fine of up to 300,000 francs.
[203] Hiti, M. H. M. *Information Crime: Models of Its Applications*. 2nd ed. Dar Al-Kutub Al-Qanuniyya, 2014. p.16.

capturing electrical waves. It takes the form of collecting the transmitted information and converting it into readable information or recording it. The perpetrator of interception does not predetermine the specific information they will intercept but rather learns about the content of the electronic message through the techniques employed after it has been processed. They capture the message as it is without making any modifications and may verify its contents with the sender, or intentionally delay its delivery. Obstruction occurs through any action aimed at preventing the message from reaching its intended recipient. Modification means modifying the message and changing its content in whole or in part[204]. Either deletion is done by destroying the content of the message. The second part of criminalization is when the offender encourages another person to intercept, obstruct, alter or delete a message sent by electronic means[205].

Fourthly, illegally accessing data or information from an information system, website, or information network that offers banking services supplied by banks or financial institutions.

II.3.2.2. Criminal Consequence

Whether a result is achieved in the first and second form of attack on electronic banking data and information or not, it is the same. It's just an entrance aimed at the attack, and whether that attack came true or not doesn't matter then. The third and fourth forms are the capture, interception, obstruction, alteration or deletion of data related to electronic banking services or information sent through the information network or information system provided by banks or financial companies, as well as obtaining without authorization data or information from an information system or website. An electronic or information network in which banks or financial companies commit material crimes related to the banking services they provide, and we hope that this will result in criminal activity in it. The legislation also makes a distinction in the severity of penalties between unauthorized access that directly results in an assault and unauthorized access that leads to such an assault indirectly. Penalties are typically harsher in the latter scenario. This differentiation is based on the inherent difficulty in proving the perpetrator's

[204] Qoura, N. A. *Economic Computer Crimes: A Theoretical and Practical Study*. Dar Al-Nahda Al-Arabiya, 2003/ 2004.p.18.
[205] Ahmed, H. A. A. *Traditional and New Information Crimes and Their Applications in the Bahraini System*. 2013. p.11.

intention to cause harm. There are situations where unauthorized access, although not intended to cause harm, inadvertently results in damage or assault on the system. This outcome surpasses the perpetrator's initial intentions. The legislation fails to address this potential discrepancy, highlighting the need for nuanced penalties to account for such unintended consequences.

II.3.2.3. Ethical Pillar

Intentionally accessing an information network, information system, or website without authorization, or in violation of the license related to banking services provided by banks or financial companies, is a deliberate offense. Article 3 (a) states at the beginning of article 3 (a): "Anyone who deliberately enters ... "The intended intent is general criminal intent. A program through an information system, website or network, and the crime of deliberately accessing, publishing or using the banking service provided by banks and financial companies, with the aim of canceling, deleting, adding or information related to destruction, disclosure, damage, blocking, modifying, altering, transferring or copying. Data or information, or stopping or disrupting the operation of an information network, information system or website is also a deliberate crime, and Article (3/b) stipulates that: "If the access provided for in paragraph (a)", and this means this crime is intentional, as paragraph (c) stipulates that: "Every person shall be punished..."; the crime of entering with the intention of attacking the system, information network or website that occurs by unintentional error, and the intention of the crime is to racist with his knowledge . The offender must be aware of them and the consequent unauthorized access to the information network, information system or website. In addition to general criminal intent, there must be a specific criminal intent, since it is not enough to deliberately enter the premises. Rather, the will of the offender must be directed to achieve a certain consequence represented in the forms of abuse mentioned in paragraphs (b) and (c), the entry is for the purpose of an objective required by the legislator. The crime occurs if this is achieved, whether or not the offender achieves this objective after entry.

If the unauthorized entry is solely for criminal purposes as outlined in paragraphs (b/c), or for any other purpose, it constitutes the offense specified in Article (3/a). This offense pertains to unauthorized entry without a license, or in a manner that contradicts or exceeds the permit. The act of interception, obstruction, alteration, or deletion of data or information transmitted over the network through electronic banking services provided by banks or financial companies,

whether it occurs mistakenly or intentionally, requires general criminal intent. Similarly, the offense of obtaining data or information without permission from an information system, website, or information network that provides banking services to banks or financial companies falls under this category.

II.3.2.4. Punishments

Among the penalties imposed on perpetrators of crimes mentioned in Articles (6 & 7) (electronic banking operations crimes) of the Jordanian Electronic Crimes Law, as they are electronic crimes, are the seizure and closure of the place where the crime was committed. Seizure means the confiscation of property proven to be linked to the committed crime and adding it to the state's assets. On the other hand, seizure can be a complementary penalty when applied to something that may be possessed or traded, to complement the original penalty and rule on it in this case. Seizure is a precautionary measure when applied to something considered to be possessed or traded, which falls under the jurisdiction of the court, and it is considered a crime in this case, and thus mandatory.

Article 13/j of the Jordanian Electronic Crimes Law authorizes the competent court to order the seizure of devices, tools, means, and materials, and to stop or disable the operation of any information system or website used in the commission of any of the crimes stipulated or covered by this law, as well as the seizure of funds obtained from these crimes and ordering the removal of the violation at the expense of the perpetrator. The penalty is also doubled in case of repeated commission of any of the crimes listed in the Electronic Crimes Law, including, of course, crimes related to electronic banking operations (Article 18 of the Jordanian Electronic Crimes Law). The penalty is also doubled if committed by a person as a result of performing his duty or work or exploiting either of them (Article (8) of the Jordanian Electronic Crimes Law), The Electronic Crimes Law goes beyond the general provisions regarding criminal participation and the equality of the original and accessory penalties, according to Article 14 of the Electronic Crimes Law. Anyone who deliberately commits a crime stipulated in the law intervenes in it or incites it shall be punished. This law specifies the penalty prescribed therein for the perpetrator.[206]

[206] Articles (6) & (7) & (8) & 13/j & (14) & (18) From Jordanian of the Electronic Crimes Law.

Whoever commits the crime of assaulting banking operations with one of the descriptions mentioned in Articles (3-6) of the Cybercrime Law shall be punished by temporary hard labor for a period of not less than five years, and a fine of not less than (5,000) five thousand dinars and not exceeding (15,000) fifteen thousand dinars. [207] The penalty for attempting to commit one of the forms of crime stipulated in Article (7) of the Cybercrime Law depends on the act committed, as the crimes mentioned in Articles (3-6) are all misdemeanors as mentioned above in the judgment of attempted acts, as the criminal description of these acts changes these crimes to become crimes of the type of criminal offenses if they occur on data or information related to an attempt. Committing acts related to electronic banking operations, as stated in Articles (3-6) of the Cybercrime Law, and failure to achieve the result Although the perpetrator tries to do so according to the general rules. The penalty for attempted crime constitutes the crime of attempted crime, and the perpetrator in this case is punishable in accordance with the Penal Code, because the Cybercrime Law does not contain special provisions on attempt.

II.4. Electronic Banking And Money Laundering Activities

Money laundering is the illicit acquisition of substantial sums of money through unlawful operations like drug trafficking or terrorist financing, and disguising its origins to make it look legitimate. Banks and other financial institutions play a crucial role in combatting money laundering due to their widespread presence in the financial system. Financial institutions are implementing efforts to reduce the risks associated with fraud, money laundering, and other financial crimes that have arisen as a result of the COVID-19 epidemic. These measures encompass the implementation of enhanced due diligence procedures, rigorous monitoring of all transactions, and the utilization of advanced technologies such as artificial intelligence and machine learning to identify any suspicious patterns or behaviors linked to money laundering. These measures aim to bolster the anti-money laundering efforts of financial institutions. Amidst

[207] See articles 68-71 of Jordanian Penal Code No. 16 of the year 1960.

the epidemic, regulatory institutions, such as central banks and financial intelligence units, offered guidance and recommendations.[208].

Since it gives criminals the opportunity to keep money they have obtained illegally and unethically, it is clear that money laundering occurs through the various services provided by financial institutions, such as loans, investments and foreign exchange that make it a common entry point for criminals, when it comes to assessing the risks to customers, in particular, there is a dearth of studies that examine the role that individuals play in assessing the risks of money laundering. Regulatory elements, such as anti-money laundering protocols and compliance with regulatory mandates, are the main focus of risk assessments conducted during the incorporation of financial institutions. Despite the availability of automated alternatives, financial firms still rely on human assessments of money laundering risks; This is actually what one of the most important **hypotheses** on which the research was based focuses on, which states that E-banks will face difficulties in complying with several financial rules, such as anti-money laundering (AML) and know-your-customer requirements, and the need to develop comprehensive strategies to manage their transaction scenarios.

Financial organizations are very concerned about money laundering. Numerous banks face substantial fines due to shortcomings in their risk assessments related to money laundering. For instance, HSBC Bank, headquartered in London, received a fine of over $2 billion from a U.S. regulator for its failure to address money laundering activities by Mexican drug traffickers using its system. This incident prompted increased scrutiny of the banking sector's adherence to anti-money laundering laws, particularly concerning the role of international banks in facilitating illegal financial activities. Another case involves Standard Chartered Bank, which resolved allegations of violating U.S. money laundering regulations in its dealings with Iranian customers by paying a $340 million settlement to a U.S. regulator. The significant financial repercussions faced by these banks have undoubtedly had a broad impact on the overall financial system. Consequently, there is widespread questioning regarding the flaws in these banks' risk management systems, particularly in their evaluations of money laundering risks. Had bank employees exercised greater caution in assessing the possibility of money laundering, losses

[208] Supriyanto, E. E., Tunda, A., and Upe, A., eds. *Global Policy in Dealing with the Covid-19 Pandemic*. First Edition. Kendari: Romah Boni, 2021, p. 17. "Opportunities for Implementing e-Rupiah Policy Innovation in Financial Transactions in the Covid-19 Pandemic.

might have been avoided. The Central Bank of Jordan has determined a financial transaction exceeding twenty thousand Jordanian dinars or its equivalent in foreign currencies. Financial transactions below this threshold and evidence indicating that they are interconnected transactions are considered a single financial transaction.[209]

"Electronic banks face critical issues in increasing employees' knowledge and providing them with appropriate anti-money laundering training, appropriate training is essential to ensure that employees are aware of the risks and rules and their role in stopping this practice, the designated bank is responsible for issuing instructions and keeping employees up to date with technical developments, scenario-based trainings can help employees practice detecting and responding to suspected money laundering activities, clear reporting methods, employee engagement and safeguards should be established to prevent financial crimes, Personal training through technology-based modules and simulations can ensure effectiveness and relevance, interdepartmental communication and cooperation must be strengthened to promote anti-money laundering measures Cooperation with industry and law enforcement associations can help design more comprehensive and ethically sound training programs, electronic banks can empower their employees to combat money laundering by promoting a culture of compliance and providing comprehensive training, and a comprehensive and advanced training program, along with technology, can help evolving and robust regulatory frameworks, in reducing the likelihood of financial crimes in the electronic banking sector[210]. "Previous studies have shown that workers do not always possess the capabilities required to perform their professions appropriately. Their ability to assess risk within a company may be influenced by internal and external factors, such as how well the control systems work and if the necessary technology is available, the level of efficiency is one of them.[211] in fact, what was mentioned above indicates and confirms one of the most important **hypotheses** on which this research was based, which proves the importance of this hypothesis regarding the additional qualification requirements

[209] Central Bank of Jordan, annual report (2021). Appendix No. (2/A).
[210] suspicious indicators of money laundering operations. Basel Committee on Banking Supervision (BCBS). Basel III framework: Regulations and guidelines aimed at enhancing regulation, supervision, and risk management within the banking sector, addressing anti-money laundering considerations.
[211] Simwayi, M., and Wang, G. "The Role of Reporting Officers in Combating Money Laundering in Zambia." *Investment Compliance Journal* (2011), p. 51.

necessary for employees working in electronic banks in relation to preventing involvement in the midst of accelerating threats such as money laundering.

It is important that frontline employees who deal directly with customers have the skills to assess customer risk levels, including money laundering risks. The specific responsibilities of employees whose job is to receive transactions in the electronic banking sector can vary according to the job title, type and size of the financial institution, the level of responsibility of the employee and the overall goal of ensuring the safety and smoothness of the processing of financial transactions. Professionals in this field must maintain flexibility and stay abreast of industry trends, given the continuous evolution of banking technology and practices. This entails adherence to internal rules and regulations governing electronic banking transactions, verification of customer identities, and compliance with authentication protocols. They must also adhere to established security measures to prevent fraud and errors, troubleshoot technical issues related to transaction processing, and provide customers with clear instructions on utilizing electronic banking services. Remaining vigilant regarding security protocols is essential for safeguarding against unauthorized access and fraudulent activities. To effectively assess the risks associated with money laundering, individuals must understand the deceptive tactics employed by money launderers. The ability of first responders to evaluate the potential for money laundering is paramount. Regulatory factors, such as compliance and internal control systems, as well as external variables like regulatory obligations, significantly influence this effectiveness. As the primary line of defense against money laundering, officers responsible for researching how financial institutions assess risk face various challenges. These challenges may include ensuring that frontline staff adequately evaluate money laundering risks and navigating evolving regulatory landscapes. [212]

[212] Favarel-Garrigues, G., Godefroy, T., and Lascoumes, P. "Bank Guards: Private Actors and Anti-Money Laundering in France." *British Journal of Criminology* (2007), p. 11.

II.4.1. Reasons For The Emergence Of The Phenomenon Of Money Laundering

The phenomena of globalization, the growth of e-commerce, the speed of financial transactions, the opening up of the world economy, the tremendous technical progress in the fields of information and communications, banking and information systems, the absence of regulatory frameworks capable of curbing this crime and the inadequate supervision of banks are all contributing factors to the exacerbation and expansion of money-laundering crime. Some of the temptations exploited by money-laundering gangs include economic openness, the proliferation of modern methods of communication, the lack of transparency in bank accounts, and the freedom to convert and exchange currencies. Another contributing factor is the emergence of online e-commerce, electronic banks, or e-banks, which have exacerbated the issue by introducing administrative complexities and opportunities for corruption. Similarly, the presence of free financial centers like the Cayman Islands has also played a role. Additionally, countries such as Switzerland and Monaco, which historically relied on bank secrecy, allowed companies, governments, and wealthy individuals to deposit their assets in environments with fewer regulatory constraints, better services (such as tax evasion opportunities), and fewer legal obstacles (such as insufficient legislation) .[213] In addition, there are laws dealing with anti-money laundering, but there are loopholes and contradictions in these regulations that may encourage criminals to hide their money. It is complicated. Similarly, if corruption spreads in all aspects of the political, legal, security, administrative, financial and economic aspects of the state, all this serves to increase the magnitude of this phenomenon.[214]

[213] Switzerland is a common choice for those prioritizing financial privacy due to its regulations that restrict banks from disclosing the identities of account holders. However, new global standards and diplomatic pressures have compelled Switzerland to relax its banking secrecy regulations in recent years. In an attempt to combat tax evasion and money laundering, the government pledged to be more transparent and to cooperate with global initiatives. As a result, Switzerland has implemented policies that include automatic exchange of financial data with foreign countries.

[214] Rashid, A. *Analytical Study of the Phenomenon of Money Laundering*. Ministry of Finance and Department of Economics in Iraq (2001), p. 26.

II.4.2. Risk Of Money Laundering In Financial Institutions

The Financial Action Task Force on Money Laundering (FATF) provides a precise definition of [215], This entity engages in the act of "processing criminal proceeds to conceal their illicit origin" in order to legitimize income that has been unlawfully obtained from criminal activities. When it comes to combatting money laundering, the Financial Action Task Force (FATF) is the preferred group for setting worldwide standards. The illicit drug trade is among the unlawful establishments that perpetuate an unending cycle of money laundering. Group members engage in illegal activities such as arms trafficking, prostitution, embezzlement, fraud, corruption, tax evasion, insider trading, and theft of aid funds. For example, the Malaysian authorities assert that drug trafficking is the primary means of obtaining illegal revenue in the country. Money laundering is intricately connected to corruption among governments, companies, and criminal organizations. The authorities deemed that there was a significant likelihood of money laundering due to various predicate crimes, such as fraud, embezzlement, illicit gambling, credit card fraud, counterfeiting, theft, forgery, human trafficking, extortion, and smuggling [216]. Malaysian authorities prosecuted a total of 94 cases with alleged winnings totaling RM1.2 billion between 2006 and 2010, up from 188 cases in 2005 with a total value of RM29.9 million.[217] According to the fraud reporting alert activated by UNOPS, several cases are currently being considered and punished in accordance with the Anti-Money Laundering and Anti-Money Laundering Act 2001. Despite the adoption of the Anti-Money Laundering Act in 2001, only a few money launderers have been convicted. Perhaps there is more time for money laundering crimes to go unpunished and without recognition than has been reported in the media and regulatory organizations[218].

[215] The acronym for this group stands for the Financial Action Task Force. With the goal of preventing illegal actions including money laundering and the funding of terrorism, this multinational governmental agency has been around since 1989. First and foremost among the Financial Action Task Force's (FATF) responsibilities is the fight against terrorist funding and money laundering. Among FATF's primary missions is the establishment of international norms and the encouragement of efficient regulatory, operational, and legislative actions in this area.
[216] Asia/Pacific Group on Money Laundering. (2007). Mutual Evaluation Report of the Asia/Pacific Group on Money Laundering on Malaysia, 1-238, Inside Malaysia. (2010). Nearly 100 money laundering cases under prosecution.
[217] INCSR Report. (2006). Money Laundering and Financial Crimes INCSR, Volume Two, 2006.p.263-354.
[218] Mohamed, Z. M., and Ahmad, K. "Investigating Money Laundering Issues and Prosecuting Offenders in Malaysia." *Money Laundering Watch* 15, no. 4 (2012), p. 421-429.

In the same context, money launderers often use banks as a tool because of their ability to take deposits, lend money and even deal in foreign currencies, in addition to that banks help in laundering illicit money by allowing accounts to be transferred or repatriated funds, and the source of these funds is often hidden or obscured. It follows that some countries, including Malaysia has anti-money laundering programs that directly target financial institutions. According to the 2014 Global Anti-Money Laundering Survey conducted by KPMG, the banking sector is particularly vulnerable to the issue of ongoing money laundering (KPMG, 2014). In light of these figures, it is clear that money laundering poses a significant threat to the financial industry, including the powers of PPATK[219] and predicate crime investigators to investigate internet laundering[220].

In another context, It is worth noting here one of the judicial rulings issued by the Jordanian judiciary; the Seventh Specialized Court of Corruption at the Amman Court of First Instance convicted six people of money laundering. In a public hearing, the court handed down its verdict, which included a three-year prison sentence for the six convicted criminals and restitution. Four million dinars from one prisoner and twelve and a half million dinars from the other, a verdict that can be appealed to the competent court, the US resident was convicted of violating American copyright by creating fake electronic discs, according to the indictment. Rumor has it that he stole up to fifty million dinars, in the United States, he was fined $1 million, sentenced to 60 months in prison, and his citizenship was withdrawn, based on the verdict that this person set up companies in his son's name after his release from prison, and he started talking to two people in Jordan - a government employee and a private citizen - and began sending money to a group of other people. They are obliged to transfer them to the second party concerned. It turned out that the total money transferred by the American citizen amounted to 12.5 million dinars and he requested that part of this money be sent to an individual so that he could buy real estate in Jordan on his behalf. Two apartments and a plot of land were purchased for small amounts, with the money transferred in installments. Its total revenues amounted to seven million dinars. The banks involved in receiving these transfers had a large number of them,

[219] PPATK, Financial Transaction Reports, and Analysis Center is precisely an abbreviation for that. For the purpose of preventing and combating money laundering and terrorism financing, PPATK is an Indonesian government organization that receives, analyzes, and disseminates reports on financial activities.
[220] Anwar, M. *Urgent Need for Money Laundering Regulations Reform in the Digital Age*. East Asia Journal of Multidisciplinary Research (EAJMR), 2 (7), (2023), p.11.

which is commensurate with their income, they informed the Money Laundering Unit of the Central Bank of Jordan, which referred the file to the Integrity and Anti-Corruption Commission, which began investigating it and referred it to the competent authorities, and before the competent court after referring them to the court, six people were convicted and sentenced to three years under probation. The value of four million dinars was also seized from the balance of one of the defendants and a number of American properties, and the value of twelve and a half million dinars was confiscated from the funds of the remaining defendants detained in banks and official institutions [221].

The Central Bank of Jordan has identified suspicious money laundering activities through several indicators. These include instances where a customer maintains multiple accounts and deposits large cash amounts in each, which collectively exceed what would be expected based on their legitimate business activities, except in cases where maintaining multiple accounts is justified by the nature of the customer's work. Additionally, suspicious accounts may be characterized by transactions that are inconsistent with the customer's stated activity, such as receiving or distributing large sums of money for unclear purposes. Another red flag is the maintenance of accounts across multiple banks within a single geographical area, followed by transfers of balances from these accounts into a single account, which is then used to transfer the accumulated funds out of the country. Moreover, suspicious activities may involve the deposit of large checks from third parties into the account, with amounts that do not align with the account holder's known relationships or business activities [222].

Financial institutions must proactively combat money laundering by implementing measures to detect and prevent suspicious transactions to identify potentially suspicious transactions indicative of money laundering, these institutions need to establish guidelines as Legal regulation that protects electronic banks and customers and leads to electronic financial stability

In fact, what was mentioned above indicates and confirms one of the most important hypotheses on which this research was built, which proves the importance of this **hypothesis** regarding

[221] Seventh Specialized Anti-Corruption Court in the Amman Court of First Instance. Six individuals were convicted of money laundering and the recovery of over 16 million dinars. Petra Magazine Bulletin, November 9, 2023, in Amman, Jordan. More details are available on the website, accessed December 11, 2023, from [URL]. https://cutt.us/prtVt .

[222] Report issued by the Central Bank of Jordan for the year 2021 regarding suspicious indicators of money laundering operations and its dissemination to Jordanian banks.

Regulators face greater difficulties in protecting the security of customer accounts and assessing the potential systemic risks associated with electronic banks, in light of the question of the responsibility of electronic banks towards customers as a powerful and dominant party.

Various Jordanian financial institutions employ unique methods to monitor for money laundering, with some still relying on human monitoring despite others transitioning to fully automated systems. Automated monitoring solutions encompass a wide range, with some tailored for larger financial institutions and others designed to meet the needs of smaller banks. However, automated approaches have their limitations. For instance, the current system lacks standardized methods for assessing money laundering risks, and smaller banks may lack the resources to fully implement automated systems. *Cocheo* emphasizes [223] that "manual" (human) expertise is necessary for automated solutions to avoid false alerts and other noise. Sometimes, the data generated by the system can be fairly huge, and people are required to understand this data. Checking whether the algorithm has identified cases that may be indicative of money laundering requires human intervention.[224]

Since the money is transferred digitally, it is impossible to trace its true origin, unlike internet laundering activities. The three steps of "mode", "layering" and "integration" are typical for traditional money laundering as well as internet laundering. However, all three steps are performed using intermediate computer networks in Internet laundering. Thus, law enforcement agencies must be prepared with the knowledge of computers, money and the law in order to avoid internet laundering crimes. Unfortunately, the current rules do not clearly govern the powers of agencies in the anti-money-laundering regime.

II.4.3. Money Laundering Risk Assessment

Risk assessment is crucial for e-banks, as all banks are susceptible to money laundering given the inherent nature of banking services. E-banks engage with both current and prospective

[223] Includes articles by Steve Kociu. Steve Kociu was a financial journalist for over 40 years, having worked in publications such as Banking Exchange and ABA Banking Journal. He currently serves as the Chief Executive Editor at The Financial Brand.
[224] Roussanov, J., and Budovushkin, Y. "*Money Laundering in the Modern Crime System*." Money Laundering Monitor (2021), p. 13.

customers during financial activities such as account opening, savings, withdrawals, and transfers. It is the responsibility of reception desk staff in banks to conduct risk assessments. When evaluating the consumer risk factor, frontline officers are required to utilize their intuition and personal judgment. The daily responsibilities of frontline staff encompass evaluating the risk level for each client, assigning them a ranking, and ultimately determining the processing of their requested financial transactions[225]. One should use their own data as a starting point to assess risk and bridge the "knowledge gap" by integrating the experiences of others in light of the perceived differences between them. How people and organizations make decisions is explained by the psychological concept of judgment and decision-making (JDM),[226] in accounting, JDM research aims to assess the quality of judgment, describe the judgment process, identify variables that affect judgments and their interpretations, create and testing hypotheses about basic cognitive processes and decision-making techniques and improving the decision-making skills of individuals responsible for decision-making, include auditor data preparers and end-users of financial statements; although, JDM has been extensively studied in auditing, finance, and management accounting, and it has received surprisingly little attention in risk assessment and other branches of accounting.[227]

The Egon Brunswick lens model has been widely used by many writers since its publication in 1952 to explain human judgment and behavior. From a theoretical perspective, Brunswick recognized that human judgment occurs in a world filled with significant environmental uncertainties, relying on limited information and an individual's perspective on the issue at hand. In the lens model, Brunswick refers to environmental uncertainty using the term "signals," which in the context of research on fraud often denotes warning signs or fraud indicators. Officials in financial institutions tasked with assessing the potential for money laundering must

[225] Kouchi, S. "*Finding the Rotten Eggs at the Right Price."* Compliance Clinic (2010), p. 44-46.

[226] The subfield of psychology known as "Judgment and Decision Making" (JDM) studies the processes by which individuals and groups evaluate data, draw conclusions, settle on courses of action, and learn how individuals make decisions in various situations using experiments, survey studies, and other methods in JDM. This field integrates ideas from economics, psychology, and other fields to understand the cognitive processes and variables that influence decision-making. Individuals and organizations can enhance the quality of decision-making or develop treatments to combat cognitive biases by gaining a better understanding of the cognitive processes and biases that affect decision-making.

[227] Youssef, A., Z. M. Sanusi, M. N. Hanifa, and B. A. Barnes. "*Money Laundering Risks from the Perspectives of Bankers and Regulators*." In Seventh International Conference on Financial Crime and Criminal Justice, Wadham College, Oxford, United Kingdom, 2015. p. 7.

possess the mental acuity to identify signs that may be indicative of a potential money launderer.[228]

In the context of fraud detection, the term "signal" is commonly used to refer to potential warning indicators or indicators of fraudulent behavior. In order to prevent money laundering, financial institutions, especially those involved in online banking, need to look for certain signs. The term "money laundering" refers to the practice of transferring illicitly acquired funds through channels such as foreign banks or seemingly legitimate businesses in order to conceal their true origin.

Employees of financial institutions usually need training in cognitive detection of warning signs in electronic transactions that may indicate possible money laundering, such as suspicious account activity, strange transaction patterns or other indicators. In order to identify cases of online banking fraud, technological means are essential. In order to detect irregularities and trends in online purchases, sophisticated analytics, machine learning algorithms, and artificial intelligence systems are used. Financial institutions can use these technical tools to filter vast amounts of data for potential indicators of money laundering. Strict anti-money laundering (AML) requirements require financial institutions to have robust systems in place to detect and prevent money laundering. Both the integrity of the financial system and compliance with regulations need the ability to recognize indicators of money laundering.

Officials working at banks that offer online banking need to be adept at spotting red flags that could mean money laundering is possible. This requires both human intuition and cutting-edge technology to scan electronic transactions for signs of fraud. When assessing the potential for financial crime in an online banking environment, users' requirements to navigate and understand complex information are aligned with the lens model's emphasis on signals.

Research on JDM (Judgment and Decision Making) literature supports the theoretical foundation based on behavioral choice theory. This theory highlights that the primary focus should not just be on individual decision-making processes but also on educating people to make

[228] Kute, D. V., Pradhan, B., Shukla, N., and Alamri, A. "Deep Learning and Interpretable Artificial Intelligence Techniques Applied to Money Laundering Detection: A Critical Review." *IEEE Access*. Advanced online publication, 2021. p. 14.

more informed evaluations. Behavioral decision theory and other established decision-making theories stress the importance of considering all relevant factors when choosing a course of action. Einhorn and Hogarth's (1981) research in accounting shifted the focus from behavioral aspects to cognitive aspects of decision-making. This comprehensive approach includes various factors influencing a person's decision-making process, whether internal (such as personal traits) or external (such as their environment, job, or workplace).[229]

In the same context, the Central Bank of Jordan provides banks with key indicators related to remittances, including frequent or large transfers to or from countries experiencing political or security turmoil, repeated or substantial amounts sent to individuals in regions known for criminal activity, or incoming transfers to or from individuals without a clear connection to the customer. Other indicators include the presence of fixed payment orders without specifying the relationship between the sender and the beneficiary, transfers to and from countries known to support terrorism, or the use of multiple accounts to gather funds and subsequently transfer them to individuals or commercial entities, particularly those in high-risk areas.[230]

On the other hand, the use of cryptocurrencies may lead to a range of crimes in the electronic banking sector, affecting areas including national security, the economy and the law, according to the country's legal system. Given the possibility of using digital signatures and fake identities to use cryptocurrencies, the emergence of new methods of money laundering activities is one of the negative consequences. The goal is to use virtual information-based money, which has no physical form, to hide the source of funds and the details of the transaction technique. In illegal money laundering operations.[231]

The path to competence is the acquisition of knowledge, skills, and techniques to identify, evaluate and improve one's behavior while doing their job.[232] Employees of banking institutions remain incompetent when it comes to recognizing the threat of money laundering, and many of

[229] Wronka, C. "*Cyber Laundering: Changing Money Laundering in the Digital Age*." Money Laundering Watch (2022), p. 8.
[230] Central Bank of Jordan, (2018). Annex (2/b): Indicators of Suspicion of Terrorism Financing Operations.
[231] Sahrouni, A., and Redi, A. "Virtual Currency (Bitcoin) as a Money Laundering Tool." *ICLSSEE*, May 06, 2023. p. 14.
[232] Harding, N., and Troutman, K. T. "Enhancing Auditor Efficiency Assessments: Another Look." *Auditing: A Journal of Practice & Theory* 28, no. 1 (2009), pp. 53-78.

the gaps in our current understanding of money laundering that he has identified may be filled with a well-focused investigation.

Given the ever-changing nature and severity of risks associated with money laundering crimes, it is essential for bank employees to have access to the latest information to conduct appropriate risk assessments. These assessments include the ability to accurately draft Suspicious Transaction Reports (STRs) and other necessary skills. Interviews reveal that the capabilities of frontline officers are a significant concern, as they serve as the "first line of defense" in identifying potential money laundering cases. All interviewees emphasized that if frontline officers fail to detect money laundering risks, it can cause substantial harm. For instance, if a customer opens an account in an online bank and the frontline employee overlooks associated money laundering risks, the account is unlikely to be canceled or terminated (CO1). Once the account is opened, the damage is done, and the risks are absorbed by the bank (CO2). Frontline employees must report any suspicions of money laundering to the relevant authorities, such as the BNM, via STRs. These reports must not be disclosed to the customer, as doing so would constitute a serious regulatory offense (SE1). Therefore, the ability to conduct customer due diligence (CDD) and recognize warning signs of potential money laundering is crucial for frontline officers. It is vital for bank tellers to understand their customers personally, beyond meeting corporate standards. This understanding is part of what sets them apart in risk assessment. Financial institution cashiers should be alert to red flags and thoroughly investigate customer backgrounds since each customer may present "threats, vulnerabilities, and consequences" (SE1). To enhance these skills, all commercial banks surveyed have implemented a policy requiring all employees, including those in frontline positions, to undergo and successfully complete anti-money laundering training. This training allows frontline officers to sharpen their skills and reinforces that ignorance of money laundering threats is unacceptable; thus, everyone should complete the training session (CO2).[233]

[233] Gholam, M., Lolland, A., Hosby, R. B., and Ånonsen, J. "*Detection of Money Laundering Transactions Using Machine Learning for Money Laundering*." 2020, p. 18.

II.4.4. IT Framework For Money Laundering

Utilizing decision-making aids has been linked to enhanced performance, and prior studies have demonstrated that risk assessment, when backed by IT infrastructure, is more effective in surpassing unsupported human judgment when utilizing same signals. An organization's information systems, which are components of their IT infrastructure, may be utilized to evaluate risk. The three commercial banks utilize NORKOM Technology and Oracle's MANTAS software as a unified IT system for monitoring transactions. When new clients are recruited, databases like Banker's Equity, World Check, and Dow Jones are utilized for the purpose of screening. "Banks could not link money launderer points using the old method" (CO1), proving that these IT systems are not suitable for managing the risks associated with money laundering. Therefore, it is essential that frontline officers (E-banking employees) are familiar with IT systems and understand the data they provide. Frontline police officers may find this particularly difficult because they are not always ready or able to learn how to use new technologies, in fact, what was mentioned above indicates and confirms one of the most important hypotheses on which this research was built, which proves the importance of this **hypothesis** regarding Additional qualification requirements are needed for employees working in electronic banks related to preventing involvement amid accelerating threats such as money laundering; An individual's lack of IT expertise among workers will increase risk management costs, according to one respondent (CO3). However, the cost of IT infrastructure can be high. The purchase or development of information systems and databases requires the allocation of funding from financial entities. The larger and better the bank's IT infrastructure, the better it will be financially, which could lead to substandard management of the risks associated with money laundering," (CO2) If smaller financial institutions choose to build their own systems in an effort to keep costs low, another costly headache for financial companies is training employees to use new databases and systems. Due to the lack of knowledge of the IT architecture and the weakness of risk assessment capabilities, money laundering concerns may not be detected, in order to manage risks effectively and financial companies must increasingly benefit from IT infrastructure, more than ever, they are willing to pay money for IT infrastructure because the benefits outweigh the costs. Electronic banks consider their IT

infrastructure to be crucial in the fight against money laundering, as advanced systems can be more effective in analyzing risk". [234]

II.4.5. Money Laundering Compliance Management Processes

The banking sector has recently established a specific department to oversee the rules of AMLATPUA and other regulatory agencies and ensure compliance with them. Given the increased responsibilities and expertise required for a better risk assessment, Bank officials are now expected to incorporate compliance best practices into their day-to-day work. The "compliance function is the second line of defense" (CO1) that determines the potential for money laundering can be implemented. Compliance officers can identify potential fraudulent customers if frontline officers fail to notice the risks of money laundering. If frontline officers hadn't pre-screened customers with urgent money laundering risks, analyzing transaction compliance management would have been more difficult. In their common fight against money laundering, compliance management and frontline police must cooperate. It is standard practice within financial institutions to notify the Compliance Department whenever the FIA detects any suspicious transactions or activities at the Central Bank, and before submitting any suspicious activity or transaction to the FIS, it must first go through the Compliance Department to see if "it should be assessed whether it is genuine and warrants risk monitoring" (CO3). Any cyber banking official can submit their paperwork to FINS, but it is likely that some banks have found a way to circumvent the regulations set by the Compliance Department. In this specific case, "the number of STRs submitted to FINS is large and low-quality as they are not pre-evaluated by the Compliance Department" (SE1). A fully staffed workforce and employee training should be a top priority for compliance management if it is serious about improving its capacity and expertise, in fact which was mentioned above indicates and confirms one of the most important hypotheses on which my research was built, which proves the importance of this **hypothesis** regarding Additional qualification requirements are needed for employees working in electronic banks related to preventing involvement amid accelerating threats such as money laundering

[234] Gerbrands, F., Unger, B., Getzner, M., and Ferwerda, J. *The Impact of Anti-Money Laundering Policies: An Empirical Network Analysis.* EPJ Data Science, 2022 .p. 20.

one respondent expressed concern about the inability of staff to prepare high-quality STR reports, resulting in misleading and insufficient data (CO2). [235]

II.4.6. Legal Obligations Required For Money Laundering Operations

There should be less conflict between the drive to maximize profits for shareholders and prudent risk management under regulatory supervision, as the two can be involved in the pursuit of profit by financial institutions. As the main regulatory authority for financial institutions, the Central Bank of Jordan is responsible for a wide range of functions, including managing money laundering risks. Bank employees must go the extra mile because the authorities monitor their performance, believing that the level of compliance with regulatory requirements by financial companies is affected by the ongoing supervision of the regulatory authority, and every member of the frontline police force should be well aware of the regulations governing their work. Failure to do so may result in inadequate risk assessment and "banking institutions may punish employees on the basis of negligence" (CO2), and it may be difficult for the CBJ to pursue prosecutions over money laundering allegations due to the fact that "most cases of money laundering are not direct" (SE1). If the prosecution has been arguing about the strength of the cases for more than two years, it means that the evidence-gathering process has been lengthy, because money launderers are experts at knowing when and how to break the law, and regulators have to go one step ahead of them by understanding their distorted logic. Because money laundering is inherently linked, the authorities would benefit from identifying patterns and arresting perpetrators by revealing their "wet laundry". This is not an easy task, but it can be productive. [236]

There is information that two large UK banks have recently stopped dealing with small and medium-sized businesses (SMEs), The Economist has found a similar trend on a global scale, and the reasons for this trend are multifaceted, some of these issues include lack of incentives

[235] Dubois, K., and Gleeson. "*Money Laundering with Cryptocurrency: Open Doors and Regulatory Dilemmas*." Journal of Financial Crimes (2020). p. 13.
[236] Gilmour, P. M. "*Revisiting the Anti-Money Laundering Framework: Legal Critique and a New Approach to Anti-Money Laundering*." Journal of Financial Crime (2022), p. 25.

to operate as correspondent banks, information inconsistency, standard fines for non-compliance, increased regulatory restrictions and auditing, more complex schemes may also result from international efforts to strengthen due diligence procedures and anti-compliance systems. Money laundering, aimed at siphoning illegally obtained funds from banks, often leads to a "cat game" between perpetrators and financial institutions. This perpetual cycle of attempts and countermeasures has heightened global interest in the issue. Financial institutions, to avoid unnecessary risks, might consider refraining from non-essential transactions, especially in the current economic climate. Media, policymakers, and regulators advocate for a risk-based approach to managing customer interactions rather than eliminating risk entirely. However, conducting thorough due diligence and customer monitoring is costly, and banks often reject potentially profitable opportunities, particularly when dealing with smaller countries. The situation becomes even more complex when considering the myriad factors influencing the costs and risks for banks. For instance, financial institutions in developing countries might be reluctant to establish correspondent relationships with electronic banks, complicating efforts to combat terrorism financing and money laundering. This reluctance is particularly problematic as it can leave small and medium-sized enterprises (SMEs) unsupervised. Making simple recommendations can be challenging; in fact, what was mentioned above indicates and confirms the main hypotheses on which my research was built, which proves the importance of the **main hypothesis** regarding there is an inverse relationship between assessing potential systemic risks associated with electronic banks and developing risk management procedures to ensure financial stability amid the growth of the cyber insurance market, and regulation to reduce risk the topic of cyber insurance for electronic banks will be expanded in the next chapter in a comprehensive manner now we will discuss the first part of it, which is concerned with the inverse relationship between risk management and the development of its procedures; for example, despite apparent difficulties, Jamaica's anti-money laundering and counter-terrorism financing framework is highly regarded. For example, Correspondent banks have noted that there are no significant regulatory issues in Jamaica that would increase the risk of doing business with SMEs there. This highlights that, despite common challenges, effective frameworks can mitigate the risks associated with financial transactions in specific regions.[237]

[237] Schmid, J. *What Is the Extent of Sufficient Anti-Money Laundering Efforts? The Jamaican Experience*. Report No. IDB-PB-242. In Inter-American Development Bank's Country Policy Briefs, 2015. p. 9.

On the other hand, over the last three decades, anti-money laundering legislation within the European Union and globally have gotten progressively intricate in the context of combating money laundering. The Financial Action Task Force (FATF) is widely regarded as the most prominent international organization in developing financial policies. However, there has been not clear of agreement among European Union members over the definition of money laundering for a considerable period of time. It is important to mention that the initial anti-money laundering directive stated that money laundering is "prohibited" but not explicitly considered a crime. However, the primary goal of the EU's anti-money laundering policy was to make it a criminal offense. The Anti-Money Laundering Directive, which was included in the first directive, confirms that money laundering is effectively treated as a crime in all member states, although there is no standardized definition. EU legislators took this choice at the time because they considered it was preferable to delegate the responsibility of criminal legislation to individual member states. Nevertheless, the EU's approach to harmonizing criminal law underwent a significant shift with the implementation of the 2009 Lisbon Treaty. This treaty established a solid legal foundation for the harmonization of criminal law, including key aspects such as legal principles, criminal process, and substantive criminal law. Nevertheless, the rhetoric of "prohibition" persisted in the fourth anti-money laundering directive, which was enacted in 2015. In this directive, the legal foundation for the directive was Article 114 TFEU, which pertains to the internal market, rather than Article 83 TFEU, which deals with minimum standards for criminal offenses. and sanctions).[238]

Critics noted The fourth anti-money laundering directive did not provide clear guidance on the specific sanctions that should be imposed for this form of money laundering, and it created confusion regarding the distinction between administrative, criminal, and criminal law aspects. Nevertheless, the directive is a crucial measure in addressing the ambiguity resulting from the absence of a precise definition, and this ambiguity might potentially have negative implications from a human rights perspective. The absence of a universally acknowledged definition of "money laundering" and its correlation with the classification of the offense as administrative or criminal has impacted both the punitive and preventive measures implemented by the European Union to address this crime. This includes the third anti-money laundering directive,

[238] For further details, see Article 1(2) of Directive (EU) 2015/849 issued by the European Parliament and the Council, OJ 2015 L 141/73.

which adopts a distinct "risk-based approach". It is often essential to implement these measures, as regulated financial institutions are obligated to declare and scrutinize substantial sums of money. [239]and the Financial Investigation Unit of each Member State is notified of any suspicious transactions, FIU.net is also used to transfer information between financial intelligence units,[240] the three-pronged approach to the points system forms the backbone of the EU Anti-Money Laundering Initiative, Constituent [241]elements) officials responsible for preventing money laundering who oversee the implementation of the framework by regulated entities in the financial sector; financial intelligence units whose mission is to research or investigate suspicious transactions; institutions of law enforcement agencies with the power to prosecute; we may note that there is more than just a lack of consensus on what constitutes money and money laundering. In the interaction of these three pillars, the objectives of anti-money laundering laws are vulnerable If the independence of financial intelligence units and anti-money laundering supervisors is threatened.[242]

The survey of the structure of EU financial intelligence units (FIUs) raises questions about their operational independence. Despite being part of government structures in 10 different countries, many EU member states are subject to enforcement power; for example, the FIU is integrated within the Central Bank of Italy, the Tax Service of Hungary, and the Intelligence Service of Bulgaria. In fifteen countries, the central bank is responsible for anti-money laundering (AML) and banking supervision, while in another eleven, a distinct financial conduct authority handles this task. Consequently, over half of the EU's central banks bear the primary responsibility for combating money laundering. The independence of authorities from government influence is crucial, though other structures can also be effective in different contexts. Banks generally have the ability to determine the validity of transactions and are responsible for notifying authorities if they identify suspicious activity. However, there are instances where these guidelines are not adequately followed, which may compromise the critical function of AML supervisors. Should the independence of central banks be compromised or things not go as planned, the EU has a

[239] Directive 2005/60/EC issued by the European Parliament and the Council, OJ 2005 L 309/15.
[240] Currently, cooperation between national financial intelligence units is subject to Articles 51-57 of Directive (EU) 2015/849 issued by the European Parliament and the Council, OJ 2015 L 141/73.
[241] For a detailed overview, refer to Joshua Kirschenbaum and Nicolas Véron, "A Better European Union Architecture to Fight Money Laundering," Bruegel, https://www.bruegel.org/2018/10/a-better-european-union-architecture-to-fightmoney-laundering/ 2018, accessed March 25, 2020.
[242] Article 32(3) of Directive (EU) 2015/849 issued by the European Parliament and the Council, OJ 2015 L 141/73.

contingency plan. The European Banking Authority (EBA) can independently investigate violations of EU law, ensuring a backup measure to maintain oversight and enforcement. [243] This report concludes by noting that the independence of the Financial Intelligence Unit (FIU) has been undermined, and there are repercussions for more than just the nation including the Anti-Money Laundering Authority. The reason for this is that the most complex cases of money laundering involve many jurisdictions, according to the literature on the subject, there are three steps to the money laundering process; i) deposition; criminals deposit illicit funds in banks through banks, casinos, stores, exchange offices or other legal entities that are used to handle large sums of money discreetly: such as taxi companies or restaurants. B) "classes", a process that is carried out in them the concealment of the source of funds, often through a series of transactions. C) integration, which entails the return of dirty money to the real economy, each step can be carried out in a separate jurisdiction thanks to the single market.[244]

One of the primary challenges encountered by electronic banks is the need to enhance employee knowledge and equip them with adequate training on anti-money laundering measures. It's widely acknowledged that employee awareness and expertise play pivotal roles in the efficacy of anti-money laundering protocols. Yet, in the absence of proper training, employees might overlook or neglect to report suspicious activities, resulting in loopholes within the system. Adopting a holistic approach involves developing and overseeing anti-money laundering training initiatives for all staff members, ensuring they comprehend the associated risks, regulations, and their individual responsibilities.

To halt this practice, the designated bank must issue directives mandating the use of electronic banking and keep employees updated on technical advancements through frequent updates and refresher training. This includes informing them about the latest developments in financial crime, regulatory reviews, and money laundering. The bank should foster a culture where employees feel safe reporting suspicious activities without fear of retribution by conducting scenario-based training exercises that mimic real-life situations. This approach helps employees train to detect and respond to potential money laundering activities and prevent financial crimes. Establishing clear reporting methods and ensuring that employees understand the importance of

[243] See Article 17 of Regulation 1093/2010 of the European Parliament and the Council, OJ 2010 L 331.
[244] Dennis Cox, *Anti-Money Laundering Handbook.* (Chichester: Wiley & Sons, 2014), p. 14.

their participation is crucial. Safeguards must be in place to protect those who report suspicious activities, ensuring they feel secure. This applies equally to electronic banking; specialized training is required for each role, as employees in various departments such as customer service, compliance, and IT may encounter money laundering risks.

By integrating technology-based training and simulation modules, personalized training can be more effective and relevant, making employees more likely to detect and prevent money laundering in a electronic banking environment. Utilizing gaming-based simulations and interactive e-learning platforms can enhance interdepartmental communication and cooperation. Compliance and risk management are integral to anti-money laundering efforts, as are computing, data, and customer relations initiatives. Promoting cooperation and information exchange is vital for effective anti-money laundering measures. To design effective training programs, the central bank should collaborate with industry and law enforcement associations, providing guidance through shared knowledge and lessons learned. Comprehensive anti-money laundering training should emphasize ethical decision-making, educating workers on identifying morally challenging situations and resolving them in compliance with laws and regulations. To ensure compliance with anti-money laundering regulations, mechanisms must be established to continuously monitor employee performance, encourage a growth mindset through constructive feedback in both simulations and real-world scenarios, and emphasize the importance of accurate record-keeping and documentation in all compliance processes. Rewarding employees who consistently exceed expectations is also essential. Proper training on recording customer interactions, tracking transactions, and generating reports is crucial to maintaining an audit trail.

Electronic banks can empower their employees to combat money laundering by fostering a culture of compliance and providing comprehensive training. The ever-changing nature of money laundering risks necessitates an advanced and thorough training program. Along with a people-centered approach, the use of cutting-edge technology and robust regulatory frameworks can help reduce the likelihood of financial crime in the electronic banking sector. By implementing these strategies, online banks can better equip their employees to detect and

prevent illegal financial transactions, keeping pace with the evolving risks of money laundering.[245]

In light of the ongoing development and innovation in electronic payment operations and banking services, both in electronic and traditional banks, a range of risks has emerged that raise security concerns and challenge privacy. These concerns are exacerbated by fears about the regulatory compliance of electronic banks and their effectiveness, as well as questions about the adequacy of legal regulations governing the development of security standards for electronic payment service providers. The issue arises as to whether insurance on financial deposits is a sufficient regulatory measure to ensure financial security in transactions with electronic banks, given that all banks are susceptible to money laundering due to the nature of banking services. Banks deal with current and future customers during activities such as account opening, savings, withdrawals, and transfers.

This situation underscores the importance of adequately training and qualifying employees to identify and halt suspicious financial activities within their functional powers. This is particularly crucial for frontline employees who interact directly with customers and must possess specific skills and experience. The specific responsibilities of employees tasked with processing transactions in the electronic banking sector can vary depending on their job title, the type and size of the financial institution, their level of responsibility, and the overarching goal of ensuring the security and efficiency of financial transactions.

One of the most critical challenges in the implementation of electronic banking is raising the level of awareness and providing appropriate training for employees in the field of money laundering and related issues. Without adequate training, employees may fail to detect or report suspicious activities, leading to potential vulnerabilities in the system. Therefore, it is essential to establish and manage comprehensive anti-money laundering training programs that clearly define risks and methods to combat them. Additionally, encouraging employees to report suspicious behaviors without fear of punishment is crucial. This can be achieved through

[245] Lopez, M. R. "*Law Enforcement Recognizes Money Laundering Crime on a Pancasila Basis*." Edited by J. Hook. *UNISSULA* 38, no. 1 (2022), p. 24.

scenario-based training that teaches employees how to detect and respond to financial crimes effectively.

In addition to improving communication and cooperation between different departments, it is important to facilitate the exchange of information and advice through collaboration with relevant authorities. Establishing mechanisms to continuously track employee performance, provide constructive criticism, and reward excellence is also crucial. These steps will help create a more robust system for detecting and preventing money laundering and other financial crimes in electronic banking.

Chapter III

The Impact Of The Implementation Of Monetary Policies Of Central Banks

In the previous chapter, we discussed the most important financial risks that could hinder the work of electronic banks during the time period 2008-2024, to aimed to clarify the challenges facing electronic financial transactions, including new and ongoing challenges related to electronic payment methods, technical and criminal protection of electronic banking transactions, and vulnerabilities facing banks in money laundering operations. The aim is to define the concept of the challenges facing electronic banks. The previous chapter focuses on researching and in-depth examining the practical application of electronic banking services, focusing on key aspects such as electronic payment methods, technical and criminal protection of electronic banking transactions, and vulnerabilities facing banks in money laundering activities. This will help identify the challenges facing electronic banks. It will focus on analyzing the legal regulatory frameworks in Jordan and European approaches, as reflected in EU conventions, directives, and case law. In addition, the previous chapter explores the impact of international law within the framework of the open cooperation method to enhance the formulation of Jordanian transaction law regulations. These regulations must strike a balance between ensuring the security and privacy of users and promoting innovation and growth in the electronic payment industry. By achieving this balance, we can create a digital financial ecosystem that is comfortable and secure, as well as flexible enough to accommodate future developments.

In this chapter, given the concerns and risks addressed, we delve into the government policies that underpin legislation to reduce identity theft and fraud in online banking. The authorities face challenges in the electronic banking sector, How were new laws introduced to protect electronic bank customers, related to electronic banks, and the assessment of the potential

systemic risks associated with electronic banks, and does the emergence of electronic banks contribute to the growth of the cyber insurance market further, and this represents one of **hypothesis** in the research, this will be examined and confirmed through the electronic information security policies of central banks and countries in general, and government policies regulating the banking financial sector. Examine the fundamental framework of the electronic transactions law in Jordan and the many uses of the Central Bank of Jordan, and analyze how these frameworks contribute to the stability and security of electronic banking services within the region while discussing some EU and international trends in general.

Through this analytical presentation in this chapter, it is possible to reveal the extent to which different strategies affect financial stability, because these beliefs and ideologies raise the issue from different legal perspectives and economic interests. The EU model and the policies of the US Central Bank and Jordanian Central Bank reveal the extent to which restrictions imposed on financial policies can be eased. Moreover, it may provide a supportive analysis of the model of the recent crisis that occurred during the coronavirus pandemic in the EU, where economic reasons justify flexible working rules. Therefore, the contribution of the European and American orientation models in this research, namely the inclusion of the concept of due process, although both models differ greatly in theory and application, may serve each other in some specific paths and outcomes, and this represents one of **hypothesis**; Do you need Regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyber-attacks that could disrupt the financial system.

The chapter ends with the most common results between financial security policy and the principle and responsibility of electronic banks towards customers in terms of whether regulatory authorities face greater difficulties in protecting the security of customer accounts and assessing the potential systemic risks associated with electronic banks, in light of the question of the responsibility of electronic banks towards customers as a strong and dominant party, and this is what It represents the second hypothesis Noting the various results related to the challenges facing electronic banks.

During the last decade of the twentieth century, the global financial sector experienced significant advancements. This included remarkable technical improvements in the banking industry, the creation of new financial instruments, and the unprecedented interconnection of

financial markets. Despite these positive developments, the financial sector in both developing and developed countries has experienced crises that have negatively impacted their economies. Observing global economic trends reveals that banking problems were a common denominator in most countries facing financial and economic crises. Experts attribute this to the increasing banking risks, particularly those arising from credit.[246]

The monetary policies of central banks serve as the executive arm and representative of a state's monetary policy, encompassing financial operations indirectly. One of the crucial tasks in the monetary field is to ensure an adequate money supply and smooth cash flow within the economy. This involves providing sufficient funds for economic activities and implementing various monetary policies to maintain economic stability.

III.1. The Role Of The State In Monetary Policy

Contemporary states have a mixed economy, wherein market processes predominate. There exists a market economy, but the state exerts influence and regulates the circumstances of the market. Economic theories analyze the function of the state from many perspectives. Thus, modern nations operate under the dominance of market processes, meaning that no one or entity has exclusive responsibility for resolving economic issues. Economic operations are coordinated through the market, without any centralized control. The Central Bank is widely recognized as the primary institution of the monetary system. Nevertheless, the autonomy of eurozone monetary policy has ceased to exist, and the monetary policy of eurozone nations is now overseen by the European System of primary Banks, with the European Central Bank serving as its primary authority.[247]

Therefore, the analysis will identify the effectiveness of central banks' implementation of monetary policies in reducing the impact of the global financial crisis. As the official bank of the state, central banks will provide support to the government's economic policy without jeopardizing or compromising their primary objective.

---

[246] Hamad, Tarek Abdel Aal. *Corporate Governance: Concepts, Principles, Experiences - Governance Applications in Banks*. Dar Al-Jami'ah, Cairo, 2007.p. 23.

[247] Nagy, Z., *Public Finance Regulation in Light of Fiscal Constitutionalism*. Miskolc-Budapest: Central European Academic Publishing,."Theoretical Foundations of Public Finance Regulation," 2022.p.13-33.

Since the summer of 2008, the world has grappled with a severe financial crisis that struck numerous major global financial institutions in the world's largest economies. This crisis had profound and far-reaching effects, prompting governments worldwide to swiftly implement measures aimed at mitigating its impact and stabilizing the financial system, in fact, the above points to and confirms the **hypotheses** on which my research is based, one of which proves the hypothesis related to the need for regulators to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyber attacks that could disrupt the financial system.. However, despite these efforts, the crisis persisted, worsening to the point where some countries were pushed to the brink of bankruptcy. This was exacerbated by the involvement of certain banks in these countries in massive lending operations that exceeded the size of their GDP. As a result, this crisis has been likened to a financial disaster of unprecedented magnitude, comparable only to the Great Depression of the 1930s. Its enduring impact ensures it remains an unforgettable chapter in global economic history.[248] Indeed, July 2007 marked the beginning of the crisis as investor trust in the mortgage bond market began to erode, leading to a shortage of funds. The result was a flood of cash into the financial markets from central banks throughout the world, including the US Federal Reserve, the UK Bank, and the EU. A noteworthy outcome of this declining confidence was the widening of the yield differential between US Treasury bills and Treasury Euro Dollar deposits, which is abbreviated as the TED spread. As a result of the increased solvency given by US Treasury bills, investors started selling off their less secure assets like mortgage bonds. Following that, the TED spread changed to mirror the prevalent anxiety and unpredictability in international financial markets. But things became even worse in September 2008 when Lehman Brothers Bank went bankrupt. The stock markets crashed and many financial institutions, including banks, mortgage lenders, and insurance providers, went under as a result of this event's ripple effect on the global financial system. During this time, the TED spread skyrocketed, peaking at 4.65% on October 10, 2008. The TED spread's dramatic increase was a clear sign of how bad the crisis was and how widespread the anxiety and panic were in the world's financial markets. [249]

[248] Thabit, F. H. "*The Impact of the Current Global Financial Crisis on the Performance of Islamic Banks and Development*." Journal of Commerce and Economics - Sana'a University 3, no. 9 (2009), p. 22-44
[249] Ibid, p. 2.

The issues plaguing the US real estate, banking, and credit sectors have, without a doubt, extended to a vast array of US and global financial and economic operations. The situation swiftly expanded outside the United States, despite its origins there. What appeared to be an American crisis became a global crisis as a result of the single global economic network perfumed that to[250]; a sharp decline in the stock and derivatives markets, liquidity problems in hedge funds and equity funds (a decline in the values of assets, part of which was insured, which led to the detriment of insurance companies. Concerns about pension funds' capacity to meet their obligations were heightened by the fall in asset values, and governments' public debt increased as a result of financial rescue plans put in place to save many large institutions from bankruptcy. The Icelandic krone and the currencies of a number of Eastern European and Latin American nations all saw their value decline as a result of this crisis. Moreover, major currency markets experienced heightened volatility during this period. Furthermore, financial institutions began tightening credit for both companies and individuals, making it increasingly challenging to secure financing. This tightening of credit was a response to the difficult economic conditions and heightened risk associated with lending amid the crisis.

By maintaining its focus on its stated goals and developing monetary and credit policies that support those goals, the Central Bank of Jordan remains an indispensable tool for the Jordanian economy. As part of this process, Jordan issues banknotes and coins and makes sure they are adequately covered. The required components of the cash cover assets are specified in Article 31 of the Central Bank Act of 1971, as modified. Assets in special drawing rights, convertible foreign currencies, gold held by the kingdom, and securities issued or guaranteed by foreign governments, organizations, or international bodies are all part of this category. When purchased by the Central Bank, these assets will have a maximum maturity date of 10 years and will be denominated in foreign currencies.[251]

The Central Bank of Jordan holds a pivotal position within the Jordanian banking system, serving as the monetary authority in the country. Its primary objectives include maintaining monetary stability, ensuring the convertibility of the Jordanian dinar, and fostering steady

[250] Yassin, K. *Liquidity Cost Determinants in Emerging Markets and the Impact of the Global Credit Crisis: An Analytical Study of Companies Listed on the Amman Stock Exchange for the Period (2003-2008)*. Unpublished doctoral dissertation, Arab Academy for Financial and Banking Sciences, Amman, Jordan, 2010, p. 13.
[251] De Cook, R. *Central Banking*. Beirut: Dar Al-Tali'a for Publishing (1987), p. 30.

economic growth. To achieve these goals, the Central Bank of Jordan employs various supervisory methods over banks operating in the Hashemite Kingdom of Jordan. These include implementing measures such as mandatory cash reserves, legal liquidity requirements, credit ceilings, rediscount facilities, and acting as the lender of last resort, among other monetary policies. The Central Bank of Jordan utilizes several means to achieve its objectives concerning licensed banks. These encompass the control of the amount, standard, and expense of credit in order to fulfill the requirements of economic expansion and monetary equilibrium. In addition, the Central Bank oversees banks to preserve the soundness of their financial situations and guarantee the protection of depositors' and shareholders' rights.

As is well known, in 2008 the world was hit by a financial crisis described as the worst since the Great Depression, according to economists. Since the beginning of 2008, various economic indicators have predicted a recession in economic activity at the global level. Among the most important of these indicators were the steady rise in oil prices; the recurrence of credit crises in global markets; the mortgage crisis in the United States and the high unemployment rate. Commodities down in light of the expectation of a global recession, global inflation rates have recorded historic levels, as there was a general trend to increase the money supply, especially by the US Central Bank "FED", in an attempt to alleviate the US mortgage crisis. This inflation has been most robust in oil-exporting countries where foreign-exchange reserves have risen, lacking a package of appropriate monetary policies – for example, open market operations – to maintain money market and interest rate targets, so-called sterilization).

As commonly understood, the Central Bank's primary objective is to maintain monetary stability, which manifests in several key aspects. This stability includes keeping the general level of prices, or inflation, in check, ensuring stability in the exchange rate of the dinar, and establishing an appropriate interest rate structure that aligns with local economic conditions and global financial market developments.[252] The Central Bank endeavors to achieve this stability by regulating the volume of local liquidity in the national economy in accordance with the financing needs of economic activity. The significance of monetary stability lies in creating a

[252] Article 4 of the Jordanian Central Bank Law, No. 23 of 1971. (2) Mustafa, Ahmed. (2000). Monetary Policy and Economic Growth. Jordanian Banking Journal, Volume 19, Issue 5, p. 9. (3) Tawqan, Umia. (2001). Monetary Policy Aims to Preserve Monetary Stability. Jordanian Banking Journal, Volume 20, Issue 8, October 2001. p. 26-27.

conducive environment to encourage both domestic and foreign investment. This, in turn, fosters high rates of economic growth[253], leading to the creation of job opportunities for the unemployed and consequently reducing the level of unemployment within the country. [254] Thus, maintaining monetary stability is crucial for promoting sustainable economic development and enhancing overall welfare.

Understandably, The Jordanian Banking Law defines credit as the transfer of a sum of money from the bank to the client, in return for the customer's obligation to repay the principal amount together with any interest, fees, and other outstanding amounts, as well as any collateral, guarantees, or undertakings provided by the bank. Supervising the credit given by banks to their clients is a crucial operation since it has inherent hazards for the banks, depositors, and the whole economy. Central banks acknowledge the significance of credit management and enforce explicit and purposeful measures to successfully regulate it. Credit control refers to the Central Bank's utilization of certain methods and instruments to supervise banks' investments and banking facilities. The Central Bank directs these activities in line with current regulations to achieve predetermined objectives. In order to efficiently do this role, it is imperative for the central bank to possess resilient information systems. These systems facilitate the central bank in quickly collecting, analyzing, and utilizing data to ensure accurate and thorough implementation of credit control policies. Efficient credit management measures are essential for ensuring financial stability and fostering sustainable economic growth.

Undoubtedly, Jordanian banks encounter significant challenges, primarily stemming from the ongoing risks to the Jordanian economy due to the turbulent political situation in neighboring countries and the broader region. This turmoil has had a strong and adverse impact on foreign direct investment flows throughout the region, disrupting the recovery seen in foreign investment following the global financial and economic crisis of 2008. Despite increased foreign investment inflows to the region during the first decade of the millennium compared to the 1990s, Jordan has experienced negative repercussions on foreign investment, foreign trade, tourism income, and workers' remittances. The primary obstacle for Jordanian banks is the task

[253] Central Bank of Jordan. (2004). *Financial and banking system in Jordan (1964-2004) Research Department*, Amman, Jordan.
[254] Al-Wazni, K. *Banking System and Monetary Policy in Jordan During the Period (1989-1990)*. Strategic Studies, University of Jordan, (1996), p. 33.

of upholding monetary and financial stability, while also playing a role in enhancing the investment climate and fostering economic expansion. To address these difficulties, the Central Bank of Jordan adopted many steps, one of which was a 0.5% reduction in the interest rate for primary lending in 2009. This action was intended to promote economic expansion in the face of decreasing inflationary forces and the worsening global slump. The decline in Jordanian economic growth to 4% in the fourth quarter of 2009, compared to 9.9% in the fourth quarter of 2008, required the Central Bank to adopt an expansionary stance. Alongside lowering interest rates, the Central Bank of Jordan implemented a set of actions to tackle the consequences of the worldwide financial crisis. The measures encompassed the relaxation of criteria for categorizing credit facilities as non-performing and the modification of guidelines pertaining to legal liquidity for banks, specifically with regards to the interbank market. The purpose of these measures was to increase the amount of money available to banks in Jordan and incentivize them to offer more loans at lower interest rates. This was done with the aim of promoting economic growth and activity in the nation.[255]

III.2. Central Banks' Electronic Information Security Policies

Preserving the secrecy, accuracy, and accessibility of digital data is of utmost importance for every Central Bank. This involves establishing essential security measures to protect electronic information assets in accordance with applicable laws and regulations, both at the national level and inside the Central Bank. The primary purpose is to provide a secure work environment that enables the bank to fulfill its national and strategic goals while ensuring the efficiency of its services. Central Banks implement electronic information security management operations in accordance with the most advanced international standards and universally recognized norms. These procedures have the objective of safeguarding information assets and protecting them from impending hazards. This is accomplished by utilizing information security risk management procedures designed to reduce risks to acceptable levels, as well as employing monitoring and control methods to maintain continuous protection.

[255] Central Bank of Jordan. (2009), Statistical Bulletin.

" In its 2020 report, the European Council on Systemic Risk highlighted the substantial risk arising from the vast interconnections between financial organizations, financial markets, and financial market infrastructures. The interconnectivity, particularly in relation to their information and communication technology (ICT) systems, might give rise to a systemic susceptibility. This implies that cyber problems occurring at a local level have the ability to rapidly spread across the Union's 22,000 financial firms, possibly impacting the whole system. The financial industry functions without any limitations imposed by geographical borders. ICT breaches of a severe kind that occur in the financial industry have repercussions that go beyond the financial firms themselves. Moreover, they enable the transmission of regional vulnerabilities across financial networks and can lead to detrimental consequences for the stability of the Union's financial system, including the generation of liquidity and a decline in confidence in financial markets as a collective entity."[256]

The researcher believes that determining the information security requirements in the Central Bank should be based on its overarching strategy and objectives. This involves conducting a thorough risk assessment to identify the potential risks faced by electronic banking systems. It includes pinpointing threats to electronic information assets, vulnerabilities, and assessing the likelihood and impact of these vulnerabilities. Moreover, it entails considering legislative, legal, regulatory, and contractual obligations, as well as the prevailing organizational culture. Additionally, it involves understanding the objectives and requirements related to information circulation, processing, storage, transfer, and disposal. Lastly, it requires conducting a cost-benefit analysis to weigh the benefits of implementing controls and securing resources against the potential harm to the bank's operations in the absence of such controls.

Advancements in computerized financial operations have enhanced the global banking system's ability to tackle the present crisis, specifically the COVID-19 epidemic. The 2008 financial crisis resulted in the acquisition of valuable knowledge, which in turn led to the implementation of more stringent rules and enhanced readiness. However, it's undeniable that cyber challenges and threats increased significantly during the pandemic, posing a major challenge to the global electronic banking system. Malicious actors exploited the surge in online activities, including

[256] Act 3 from; regulation (EU) 2022/2554 of the European parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

remote work, digital transactions, and communication, to carry out sophisticated cyberattacks, resulting in major theft and fraud. During the pandemic, various threats intensified. Financial fraud attacks targeting banking customers and institutions surged, necessitating enhanced security measures in electronic banking operations. Incidents of data breaches, resulting in the theft of sensitive information, also escalated, jeopardizing the confidentiality and security of financial data. Ransomware attacks, where ransom demands are made to regain access to encrypted banking data or systems, witnessed a notable increase. The European Commission took proactive measures to address these challenges, recognizing the risks associated with increased digitization and electronic payments. They implemented special regulations and legal procedures within the European Union to enhance operational flexibility. For instance, Article 1 of the operational flexibility legislation outlines proactive steps aimed at mitigating the heightened risks associated with increased digitization and electronic payments:

"Increased digitalization and interconnectedness are also amplifying ICT risks, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems, high digital and connectivity."[257]

Certainly, effective defensive measures are crucial to combatting such attacks. Some malicious actors have capitalized on the current situation to disrupt global banking services through denial-of-service (DDoS) attacks or by targeting servers and networks. Additionally, fraudulent charity campaigns have emerged as a tactic for stealing money and personal data during the pandemic. Some opportunists exploit the names of reputable organizations involved in pandemic response efforts for their malicious activities. There is a case related to a fraudulent email requesting a donation of Bitcoin to the WHO Global to help ensure frontline workers have access to essential supplies and to support countries with the "weakest health systems" in dealing with the coronavirus, and within Swiss banks that are most in line with threats and challenges, for example; On its website, Credit Suisse urges its customers to stay alert to fraud by impersonating governments, companies and suppliers of goods necessary to fight the coronavirus and demanding donations: "Due to the general uncertainty surrounding the coronavirus, there is an

[257] Act1 from; regulation (EU) 2022/2554 of the european parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

increase in the number of criminals looking to take advantage of the current situation."[258] In 2017, Switzerland ranked 19th among the world's largest economies with a GDP of seven hundred billion dollars, but it accounted for $2300 billion worth of capital of wealthy foreigners, especially Germans, French and Saudis[259], According to the Boston Group. Switzerland has implemented significant measures to safeguard its financial and electronic banking sectors. The Institute for Economic Crime Investigation (ILCE) was formed in late 2000 as a result of a collaboration between HE-Arc/University of Applied Sciences, University of Neuchâtel, Swiss Police Institute, and the State of Neuchâtel. The entity dedicated to probing economic crimes has steadily expanded and broadened its activities since its inception. The ILCE now offers a wide range of continuing education courses to fulfill the responsibilities assigned to institutions. These courses entail completing assignments and participating in research projects that specifically address economic crime, cybercrime, or digital investigation [260].

In late March, European law enforcement authorities issued a warning specifically targeting counterfeit medication. According to Deutsche Welle, a news site, the police identified 2,000 websites that were advertising phony treatments for the coronavirus as part of a worldwide investigation called "Pandya." A total of around four million counterfeit medication packets have been confiscated across 90 different nations. Within the same framework, the Federal Bureau of Investigation (FBI) in the United States issued a warning on March 22nd, alerting Americans to the fact that "scammers are exploiting the coronavirus pandemic as an opportunity to unlawfully obtain your financial resources and personal data." [261]

Therefore, monetary policies worldwide must strive to tackle these challenges, now a paramount concern for the entire financial sector. The global electronic banking system should continue to bolster security measures, such as enhancing data security and encryption rigorously, adopting advanced detection technologies to identify and prevent fraud, improving identity verification procedures and user authentication, increasing training and awareness of

[258] Credit Suisse Group AG is a global investment bank and financial services company founded and headquartered in Switzerland. Its headquarters are located in Zurich, and it has offices in all major financial centers around the world, providing services in investment banking, private banking, asset management, and shared services.
[259] Access on 20 March 2024, available: https://2u.pw/Aj41m7U .
[260] Previous reference; Nagy, Z., *Public Finance Regulation in Light of Fiscal Constitutionalism*. Miskolc-Budapest: Central European Academic Publishing,."Theoretical Foundations of Public Finance Regulation," 2022. pp. 13-33.
[261] Available at: https://www.swissinfo.ch/ara/ access on 30 November 2023.

information security for employees and customers, and forging stronger partnerships with cybersecurity providers to develop integrated strategies against threats.

The economic downturn triggered by the pandemic has rippled across the global economy, with a surge in remote working from home posing heightened risks due to diminished discipline and swift transitions. Consequently, there's a rise in both internal and external scams and cyberattacks, potentially leading to data loss, theft, or system shutdowns. In response, the global banking system should enhance its capability to swiftly detect breaches and respond systematically to maintain the stability of the financial system. Central banks recognize the ongoing need for policy development, electronic regulations, and cybersecurity measures to safeguard against potential threats. A notable example of effective monetary policy response during the pandemic is seen in the actions taken by various central banks. For instance, the European Central Bank (ECB) introduced a new tool of accepting corporate credit claims as collateral amid the economic crisis, which has remained significant in eurozone monetary policy post-crisis. Additionally, to boost liquidity, central banks like the Central Bank of Hungary have broadened the scope of qualified guarantees to include corporate loans against large corporations. This enables capital debt exceeding specified thresholds to be included in the central bank's resource guarantee. Moreover, the central bank has made borrowing available to investment funds by allowing them to borrow from the central bank with unit coverage. [262]

In fact, The US central bank promptly responded to the economic crisis by announcing interest rate reductions and implementing quantitative easing measures, without specifying a financial limit. The Federal Reserve has acquired state pensions, mortgages backed by real estate, and business pensions." [263]

Each year on June 27th, in alignment with the International Day of Micro, Small, and Medium Enterprises established by the United Nations General Assembly in 2017, the Financial Inclusion Alliance acknowledged the Central Bank of Jordan as a prominent "Champion" for effectively addressing the repercussions of the COVID-19 crisis on these crucial economic contributors. Micro, small, and medium firms are essential for both economic and social growth. Upon the request of the Financial Inclusion Alliance, the Central Bank cooperated to post a blog

[262] Nagy, Z. Previous reference (2022, p. 13-33.
[263] Ibid, p. 17.

on the Alliance's website, elucidating Jordan's experience in reducing the adverse impacts of the crisis on these firms. The blog discussed the numerous steps taken by the Central Bank to mitigate the impact of the crisis on these enterprises.

These measures included injecting an additional 550 million Jordanian dinars into banks by reducing the reserve requirement ratio on deposits from (7% to 5%), lowering the interest rate by 150 basis points, and instructing banks to defer installments of credit facilities granted to affected economic sectors' customers. It emphasized that this deferral did not constitute restructuring these facilities and would not affect customers' credit scores. Furthermore, the Central Bank of Jordan initiated a program during the pandemic to support small and medium enterprises with 500 million dinars. This funding was provided to banks at a zero interest rate, with a condition that the interest rate on lending from banks to customers does not exceed 2% annually. The Jordanian government assumed the cost of any loans granted to finance employee salaries, with a loan period of up to 42 months and a grace period of up to one year. These loans were guaranteed by the Jordan Loan Guarantee Corporation by 85%. The program contributed to paying the salaries of 64 thousand employees and financing 10229 projects valued at approximately 8771 million dinars, creating about 12 thousand new job opportunities across various governorates of the Kingdom. Moreover, the blog commended the Central Bank's role in promoting digital transformation through initiatives such as allowing remote opening of electronic wallets and encouraging the use of Quick Response Code (QR) technology for commercial transactions. This blog underscored the Central Bank's pivotal role in mitigating the economic downturn's negative impacts on various sectors affected by the crisis.[264]

The researcher says that the summary of the measures aimed at mitigating the impact of the COVID-19 pandemic on the national economy, undertaken by the Central Bank of Jordan during the crisis, includes: first, deferring insurance facility premiums for workers in sectors affected by the pandemic; second, ensuring smooth cash flow by injecting an additional 1050 million dinars liquidity into banks; third, reducing financing costs within the Central Bank's

[264] The Alliance for Financial Inclusion (AFI) is a network of financial inclusion policymakers headquartered in Kuala Lumpur, Malaysia, founded in 2008 as a project funded by the Bill & Melinda Gates Foundation and supported by AusAid. Its main message is to encourage the adoption of comprehensive financial policies in developing countries to combat poverty, and the network includes more than 100 financial institutions from more than 89 countries. In 2010, the G20 nominated the Financial Inclusion Alliance as one of the three implementing partners of the Global Partnership for Financial Inclusion (GPFI).

program supporting developmental economic sectors; fourth, lowering loan guarantor commissions and expanding coverage under the sales guarantor program; fifth, devising financing programs totaling 500 million dinars to assist small and medium enterprises.

Electronic financial operations offer decentralization, allowing transactions to occur directly between customers through cyberspace without the need for financial intermediaries. While this reduces costs and streamlines agreements, it also poses challenges such as lack of oversight by monetary authorities, raising concerns about monetary regulation, money laundering, consumer protection, and taxation. These challenges stem from advancements in electronic payment systems and related technologies. Since joining the Financial Inclusion Alliance Forum in 2016, the Central Bank of Jordan has initiated the development of a national strategy for financial inclusion, focusing on six main areas: digital financial services, microfinance, small and medium enterprises, financial consumer protection, financial literacy and capabilities, and data and research.[265] The digital sector, inclusive of specialized committees and task forces from the public sector, has been established to design and construct electronic payment and transfer systems, ensuring financial accessibility across all regions of the Kingdom. Furthermore, the Central Bank of Jordan has implemented necessary changes within the legal framework and regulatory practices to support the adoption of modern financial technology and electronic transactions. These efforts aim to bolster the capacity of banks and financial institutions in mitigating risks associated with financial technology (Fintech) and cyber threats, thereby fostering a banking environment conducive to leveraging financial technology in service provision. Additionally, emphasis is placed on promoting financial literacy and raising awareness about its utilization. Alongside the activation of the electronic central system established in 2014, the Central Bank of Jordan has been implementing its strategic plan spanning from 2016 to 2024, which underwent testing to facilitate interconnection among its banks. This initiative, primarily aimed at traditional banks, serves as a stepping stone towards the introduction of digital financial services in Jordan. The year 2017 marked a significant

[265] Ianchovichina, Elena. "*Will a Return to Political Stability Solve the Economic Problems in the Middle East and North Africa*." Arab Voices Journal, November 1, 2013. p. 14.

milestone with the establishment of blockchain technology, laying the foundation for further advancements in the digital financial landscape.[266]

The Central Bank of Jordan has implemented policies aimed at activating and bolstering electronic banking services for banks. These measures are designed to incentivize investment, enhance liquidity, and foster connectivity between Jordan and the global economy. By embracing electronic financial exchange technologies, Jordan aims to avoid isolation from global economic activities and technological advancements. This strategic approach also seeks to mitigate the impact of regional crises and promote Jordanian competitiveness by facilitating the transition from traditional to digital finance. Through initiatives like supporting electronic financial transactions, Jordan aims to integrate its financial economy with global leaders in digital finance, including the European and American economies.

As global competition in electronic banking intensifies, influenced by various international factors such as the liberalization of international trade in electronic financial services and the pervasive adoption of information technology, Jordan's current policy of economic openness and liberalization, coupled with the emergence of private banks, compels local banks to adapt to new digital advancements. This adaptation entails comprehensive preparation across all levels, including ongoing training of personnel, adoption of modern management and accounting systems, particularly enhancing technological infrastructure, and exploring avenues to reduce banking service costs while maximizing returns. Central to this adaptation is the imperative to focus on the credit function of banks, given its significant impact on the overall financial position. A secure loan portfolio not only ensures high returns for the bank but also minimizes associated credit risks, making prudent credit-granting decisions essential for sustained profitability[267]. As commonly understood, electronic financial operations are marked by decentralization, meaning transactions can occur directly between customers through cyberspace, bypassing financial intermediaries. Although there are benefits in terms of cost savings and simplified arrangements, there are also disadvantages. The system functions

[266] Daniel, and Guida. "A Distributed Ledger and Shared Ledger that Provides Documentation and Verification of Transactions." 2019. & Kopylash. "A Distributed Database Operating in a Peer-to-Peer Network, Where Each Peer in the Network Possesses a Complete or Partial Copy of the Database." (2018), p. 17.

[267] Al-Daghim, A. A., and Al-Amin, M. "Al-Juro Iman: Credit Analysis and Its Role in Streamlining Banking Operations Applied to the Syrian Industrial Bank." *Tishreen University Journal for Scientific Studies and Research* 28, no. 5 (2006), p. 35.

independently from the jurisdiction of the monetary state, which raises questions regarding monetary regulation, money laundering, financial consumer protection, and taxes.

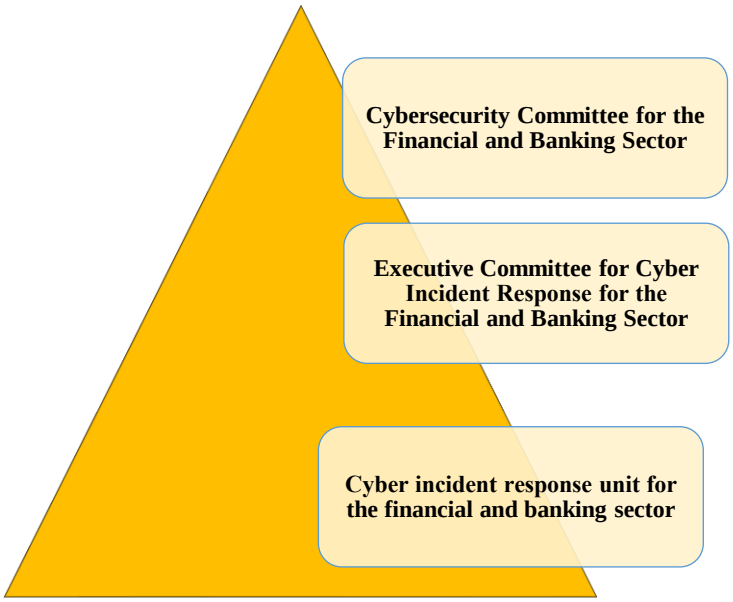
Recognizing the importance of keeping pace with rapid technological advancements and its role in maintaining financial stability, the Central Bank of Jordan has actively encouraged innovation in financial technology (fintech) and emerging digital solutions. This involves fostering initiatives across both public and private sectors to attract investments and bridge the gap between supply and demand. By empowering innovators and encouraging the development of creative financial services and products, the aim is to enhance the local and regional market with value-added offerings. The focus remains on ensuring safe and effective access to digital financial services, with robust cybersecurity measures, consumer protection, transparency, and competitiveness. As part of this effort, the Central Bank of Jordan established the financial technology innovation lab (BOX REG JO) to support the national goal of fostering a secure and competitive fintech environment, ultimately boosting liquidity flow and foreign investments[268]. The Central Bank of Jordan seeks to establish legal regulation framework that fosters innovation and development in (fintech). This includes creating an experimental environment where entrepreneurs and developers can test digital financial applications with real customers. The goal is to support innovation, enhance competitiveness in digital financial services, improve access to such services, ensure stability in the digital financial sector, and protect the rights and data of financial consumers. To achieve this, the bank has prepared a regulatory framework outlining the operational procedures of the digital financial technology regulatory lab.

Aligned with its commitment to fostering a secure investment environment in Jordan and bolstering the financial and banking sector's ability to manage cyber risks, respond to cybersecurity incidents, and safeguard the institutions under its supervision from cyber threats, the Central Bank of Jordan, in collaboration with the country's banks, initiated the formation of a cybersecurity incident response team in 2019. This team comprises the Cybersecurity Committee for the Financial and Banking Sector, the Executive Committee derived from it, and the Cyber Incident Response Unit for the Financial and Banking Sector. Their mandate involves

[268] The Organizational Technology and Innovation Laboratory (BOX REG JO) is a real, secure, controlled, and monitored experimental environment built on risk management methodology. It allows entrepreneurs and business innovators, through real clients, to conduct tests on innovative financial products and services using advanced technological solutions within clear parameters with the highest levels of transparency.

overseeing the team's operations in accordance with existing legislation, regulations, and best practices.

Figure No. (6); represented by the cybersecurity committee for the financial and banking sector, the executive committee of the cybersecurity committee, and the cyber incident response unit for the financial and banking sector at the central bank of Jordan.



Source: The official website of the Central Bank of Jordan[269] .

The Cyber Incident Response Unit for the financial and banking sector is dedicated to bolstering the cybersecurity framework of financial institutions, enhancing their preparedness to counter cyber risks. Its key responsibilities include contributing to formulating a cybersecurity strategy, overseeing program implementation, and reporting progress. It also develops guidelines for cybersecurity controls assessment, conducts security studies on potential breaches and fraud, and collaborates with various stakeholders to promote innovation and capacity-building in cybersecurity. Additionally, it serves as a central point of contact for engaging with local, regional, and international entities. Ensuring transparency and customer accessibility, the unit advocates for regular review and updating of bank and financial company websites to ensure comprehensive disclosure of products, services, and complaint filing procedures.

[269] Central Bank of Jordan. (n.d.). Official website of the Central Bank of Jordan. Retrieved from, https://www.cbj.gov.jo/Default.aspx

The Central Bank of Jordan has made commendable progress with the establishment of the regulatory laboratory, fostering an experimental environment for innovators to explore digital financial applications. This initiative aims to spur innovation, improve competitiveness, expand access to digital financial services, and safeguard consumer rights and data. While this initiative is a positive step towards encouraging investment and leveraging financial technology, in fact, the above indicates and confirms the hypotheses on which my research was based, which proves Key **hypothesis** legislation has been implemented to limit identity theft and fraud in online banking. However, authorities are encountering challenges in establishing secure and authenticated digital identity procedures. To introduce new laws to protect electronic banking customers, and ensure transparency in fees, terms and dispute resolution systems.

there remains a question of whether it is sufficient to pave the way for the establishment of electronic banks. It prompts the query as to why the Central Bank has not introduced specialized legal regulations tailored to address the unique challenges facing electronic banks and establish clear licensing conditions. Developing such regulations could facilitate the establishment of new electronic banks in Jordan, attracting external investment and fostering innovation in the electronic banking sector.

III.3. The IMF's role in strengthening Jordan's financial framework [270]

The IMF has been extensively involved in Jordan's financial sector, particularly initiatives affecting the legislation and operation of e-banking. The following is a summary of the IMF engagement and its impact on Jordan's financial industry. Jordan's financial industry has transformed as a result of the IMF's efforts to strengthen its financial framework, with growing usage of digital banking and financial technology (fintech). The IMF has contributed to these developments through policy recommendations such as digital financial inclusion, in which the IMF advised Jordan on how to use digital banking to increase financial inclusion, particularly for underbanked populations such as women and rural communities; and in its Article IV

[270] Avaliabel at: https://www.imf.org/en/Home access on 2 December 2024.

consultations, the IMF recommended policies to improve access to digital financial services while maintaining financial stability.

Jordan has received direction to match its banking rules and regulations with worldwide best practices, including e-banking. Specific areas of focus include digital bank license requirements, operational risk management, and online transaction-specific consumer protection regulations. The IMF is collaborating with Jordan's Central Bank to build robust legal and regulatory frameworks for e-banking. In terms of cybersecurity frameworks, the IMF has stressed the need of cybersecurity measures in protecting the integrity of digital transactions and preventing systemic risks, as well as advise on building legal frameworks for reporting and responding to cyber incidents in the banking sector. Recently, the IMF launched the FinTech Sandbox Initiative. The Central Bank of Jordan, with IMF advice support, has established a regulatory sandbox to allow fintech firms and e-banks to test innovative goods and services in a regulated setting. This approach has promoted innovation while guaranteeing regulatory compliance.

Jordan has made substantial progress in strengthening its anti-money laundering and counterterrorism policies under IMF supervision. Jordan's Central Bank has tightened supervision of digital financial transactions in order to prevent e-banks from being used for criminal purposes. The IMF has also encouraged Jordan to integrate its AML/CFT processes with Financial Action Task Force (FATF) standards, particularly in relation to digital wallets and online banking systems.

It is worth noting the cooperative success story: The IMF's cooperation with Jordan has yielded tangible results in terms of economic resilience, as digital financial services supported by strong legal and regulatory frameworks have assisted Jordan in overcoming economic shocks, including the COVID-19 pandemic.

III.4. Responsibility Of Electronic Banks Towards Customers

The customers face significant challenges related to guaranteeing safety and security in the face of cyber threats and fraud risks, these concerns arise from uncertainties about whether errors stem from the electronic banks themselves or from the customers' actions, to overcome these hurdles, there is a crucial need for a sense of safety and trust that can instill confidence in customers and encourage them to embrace electronic banking services without hesitation.

Customers seek assurance from electronic banks regarding their responsibilities and commitments towards ensuring the security of transactions and protecting customer data, while electronic banks primarily operate through virtual platforms with minimal physical presence, new customers are often apprehensive due to the absence of tangible references or points of contact.

It is conceivable in common law that one party to the contract is obliged to use reasonable care so as not to cause undue harm to the other party. Financial institutions are regulated to meet certain standards through civil law compliance, which is based on data protection law and compliance by design and assumption (which may be heavily influenced by algorithms). We have demonstrated that this essentially entails a promise not to capitalize on the disproportionate influence that online banks have on their customers.

It's crucial for e-banks to prevent any actions that might undermine customers' rights, even though their dominant position alone doesn't constitute a crime [271]. Given the factors leading to their dominance, e-banks have strong reasons to exercise vigilance. Similar to Article 102 of the Treaty on the Functioning of the European Union (TFEU) [272], which doesn't specify a limited set of violations applicable within the EU, dominant companies are obligated to act responsibly in case of restrictions, including a lesser degree of customer focus. Examples of such duties include legal obligations derived from institutional duties, as well as proactive measures to address violations. From the customer's perspective, this entails a commitment to act professionally and fairly. Germany's privacy ruling on Facebook in 2019 serves as a notable example, where the company's efforts to maintain privacy were deemed crucial. As an entity

[271] Case: 322/81 NV "nederlandsche banden industrie michelin v commission judgment of 9 November 1983, ECLI:EU:C:1983:313, para 57. See also Case T–228/97 irish sugar plc v commission judgment of 7 October 1999, ECLI:EU:T:1999:246, para 112; Case T–203/01 manufacture franc¸aise des pneumatiques michelin v commission judgment of 30 September 2003, ECLI:EU:T:2003:250, para 55; Case T–219/99 british airways plc v commission judgment of 17 December 2003, ECLI:EU:T:2003:343, para 242; Case C–202/07 P france te´le´com v commission judgment of 2 April 2009, ECLI:EU:C:2009:214, para 105; Case C–457/ 10 P AstraZeneca AB and astrazeneca plc v commission judgment of 6 December 2012, ECLI:EU:C:2012:770, para 134; Case C–209/10 Post Danmark A/S v Konkurrencera˚det Judgment of 27 March 2012, EU:C:2012:172, para 23; Case C–23/14 Post Danmark A/S v Konkurrencera˚det Judgment "of 6 October 2015, ECLI:EU:C:2015:651, para 71.

[272] The treaty on the functioning of the European union is one of two treaties forming the constitutional basis of the European union, the other being the treaty on European union. it was previously known as the treaty establishing the European community.

with antitrust features, it's incumbent upon the company to treat customers fairly and without discrimination, free from exploitation and bias.[273]

Determining abuse of dominance, particularly in cases involving predominantly online banks, entails recognizing not only the existence of a special position but also the understanding of this position by the electronic bank itself, given its primary focus on prevention, governance, and responsibility. Assessing dominance often involves sophisticated market definition analysis, as seen in situations involving Article 102 of the TFEU. However, this shouldn't deter from evaluating dominance. For instance, in a 2018 report to the German Ministry of Economy, *Heik Schweitzer* and colleagues argued that abuse alone could provide adequate evidence of a dominant position, potentially replacing the previous, more traditional market definition approach[274].Continuing this perspective, *Schweitzer, Kramer, and de Montjoy* recently recommended to the European Commission's Director General for Competition (2019) that it is sensible to assume that banks with either a legal or de facto monopoly, whether operating online or offline, will exert dominance and control[275]. Here, it is possible to be comprehensive with this. Any endeavor predetermined to be dominant by an authority or, ultimately, a court, is subject to the same rules. The duty of care may intersect with those provided or imposed by the dominant body, and such situations are admittedly uncommon. As is the case now for EU ECN operators, the same logic certainly applies to online banking[276]. Risk management can teach us a thing or two about direct regulatory involvement, just as it did with the GDPR. [277]

The original principles and economic rationale not only apply to damages like negligence but also, in the researcher's view, should encompass the notion of a duty of care. It would be wiser

[273] Preliminary assessment in Facebook proceeding: "Facebook's collection and use of data from third-party sources is abusive, Bundeskartellamt press release, 19 December 2017; Bundeskartellamt prohibits Facebook from combining user data from different sources, Bundeskartellamt press Release, 7 February 2019; Bundeskartellamt, Case Summary, Facebook, Exploitative business terms pursuant" to s 19(1) GWB for inadequate data processing (Decision of 6 February 2019) accessed 8 June 2019.

[274] Schweitzer and others (n 1). The same idea was advocated in 2005 by the Economic advisory group to DG COMP in the report An Economic Approach to Article 82 accessed 8 June 2019.

[275] Crémer, J., de Montjoye, Y.-A., and Schweitzer, H. *Competition Policy for the Digital Era*. European Commission, 2019. Accessed June 8, 2019. p. 22.

[276] This category is established by Article 25 of the General Data Protection Regulation (GDPR), which is a regulation of the European Parliament and Council dated 27 April 2016. The GDPR aims to protect the rights of individuals in relation to the processing of their personal data and the free movement of such data. It also repeals Directive 95/46/EC. The official reference for the GDPR is OJ L119/1 (2016).

[277] C Sunstein, Risk and Reason: Safety, Law and the Environment (CUP 2004); U Beck, Risikogesellschaft: Auf dem Weg in eine andere Moderne (Suhrkamp Verlag 1986).

for the leading online bank to implement safeguards rather than pursue individual customers for damages, especially considering that the bank already possesses all necessary information to make informed decisions. This perspective extends to various contexts, including the trustee's obligation to the beneficiary, general contract law, consumer protection laws, employment and tenancy laws, and finally, the financial services regulations governing electronic banking operations. These frameworks explicitly aim to safeguard the weaker party in contracts by addressing inherently unequal negotiation dynamics.

There was no difference between civil law and the negligent tort approach; whether or not the obligation of the duty of care is equitable may not be a point of contention between the parties. The private law test seems to have been a last-minute addition. However, it is clear that the precautions taken to avoid liability and injury will have a protective effect in professions or activities that are often subject to this criterion. The above method of regulation has its roots in regulated financial services[278], where the duty of care has evolved from the requirements of the markets under the Financial Instruments Directive and the second for online banks to keep their customers informed and updated. The definition of this is outlined in the Financial Services Act of the Netherlands. The UK's Financial Conduct Authority (FCA) has put up a comparable and uncomplicated strategy, wherein a "duty of care" is defined as the affirmative obligation placed on an individual to ensure that their activities adhere to specific criteria. This commonly pertains to the obligation to use reasonable caution and expertise when delivering an internet-based service, particularly in the realm of customer-oriented electronic banking. This development is significant due to the involvement of the FCA[279], is responsible for applying the general competition rules to the financial sector to ensure effective competition in the interest of the interest. The Financial Supervisory Authority (FCA) has simultaneous (parallel) powers with the Consumer and Market Authority (CMA), which means it is responsible for this and more. In light of the above, and in the UK as well, discussions are underway on the creation of a new independent regulator for the Internet industry. This would replace self-regulation with government authorities and is clearly relevant to cases of private tort to consumers.

[278] Busch, D., and van Dam, C., eds. *A Bank's Duty of Care*. Bloomsbury, 2017. p. 34.
[279] *FCA, Discussion Paper on a Duty of Care and Potential Alternative Approaches DP18/5 (July 2018). This article provides similar examples with regard to prospective financial services regulation in the USA and Australia*

Indeed, electronic banking operations are economically significant, being among the simplest and most cost-effective banking transactions, facilitated by straightforward yet sophisticated mechanisms. However, they entail various risks concerning the economic interests of both customers and banks, and at times, even the national economy; this is what is worth noting in one of the most important **hypotheses** on which this research is based, Regulators to face greater difficulties in protecting the security of customer accounts and assessing the potential systemic risks associated with electronic banks, in light of the question of the responsibility of electronic banks towards customers as a powerful and dominant party.

The absence of specific regulations governing the responsibilities of electronic banks conducting these operations has prompted me to delve into researching the accountability of electronic banks. This aims to streamline the process for customers seeking rightful compensation in case of damages, thereby instilling a sense of security when conducting financial transactions.

The advent of the information and communication revolution has brought about profound societal changes, with electronic banking emerging as a crucial element in economic activities, particularly in e-commerce. Given the link between banking operations in e-commerce and financial technology, safeguarding customer rights is imperative for the regularity, prosperity, and trustworthiness of these transactions. This necessitates legal frameworks to regulate electronic transactions due to their widespread prevalence.

As banks have evolved their methods and tools, there's been a noticeable shift towards digital or electronic money as an alternative to physical currency. Consequently, legal rules and theories are gradually adapting to accommodate the concepts of electronic money and its mechanisms. This has led to the enactment of laws aimed at facilitating bank administrations' handling of electronic challenges, spurred by technological advancements.

The increased volume and expansion of banking activities have amplified interest in the topic of bank responsibility. Banks, as significant economic actors, bear the duty to address societal issues, known as social responsibility. The relationship between banks and customers within contractual frameworks is not solely determined by contractual provisions but also by adherence to legal regulations set by legislators to ensure a balance of interests between parties and protect the banking sector's stability. Regulatory bodies tasked with overseeing the banking sector play

a crucial role in enforcing these rules, and any violation by electronic banks of contractual or legal provisions renders them liable to legal consequences. [280]

From the above, the European legislator realized the importance of this matter and issued a legal text in Article 5 of the Operational Flexibility Legislation, which states the following.

ITU's policy and legislative actions at the national level have not been effective in addressing ICT risks, which nevertheless provide a challenge to the operational resilience, performance, and stability of the ITU financial system. The changes implemented during the 2008 financial crisis principally focused on enhancing the financial resilience of the Union's financial sector. Their main objective was to safeguard the Union's competitiveness and stability through a study of economic, prudential, and market behavior. ICT security and digital resilience, while considered part of operational risk, have received less attention in the regulatory agenda during the financial crisis. These themes have only developed in some aspects of financial services policy and the ITU regulatory environment, or in a limited number of Member States." *[281]*

The integration of modern electronic technology into banking operations, including electronic banks, has presented numerous challenges. Electronic banks, being economically and technically proficient, often dominate their relationships with customers. This raises questions about civil responsibility for electronic banking operations is it solely the bank's, the customers, or a shared responsibility? The absence of clear regulations regarding civil liability has necessitated research to facilitate customer compensation in case of damage, instilling a sense of security and confidence in electronic banking. To address these risks and developments, monitoring risk levels and implementing effective control procedures have become imperative. In electronic banking, various risks, such as technical, fraud, operational, and legal risks, can lead to financial losses. These risks underscore the need for clear legal frameworks and robust security measures to maintain financial stability and protect customer interests in the electronic banking landscape.

---

[280] Fadel, Bani Muhammad. "*Electronic Banks: What They Are, Their Transactions, and the Problems Raised by Dealing with Them*." Journal of Jurisprudence and Law no. 39 (2016), pp. 44-53. Retrieved from [URL] http://search.mandumah.com/Record/728088

[281] Regulation (EU) 2022/2554 of the European parliament and of the council of 14 December 2022, on digital operational resilience for the financial sector and amending regulations (EC).

One of the modern risks that must be noted here is the electronic espionage trick and here the hacker spies on communications between two Internet users and misuses the data obtained in this way or intervenes in communicating directly to obtain data and information on their accounts,[282] and electronic fraud appeared for the first time in the United States and spread all over the world. It has been possible to trace the development of fraudulent cyber fraud in Germany since. [283]

The question arises whether instances of theft, plagiarism, account hacking, and opening an electronic account in someone else's name are the responsibility of the bank or the customer. The researcher contends that responsibility is shared between both parties. This is because determining responsibility becomes complex when multiple factors contribute to an outcome. Damage can result from a chain of events, where one error leads to another, and so on, known as the succession of damages. In such cases, establishing the causal relationship between the bank's error and the customer's damage requires careful analysis. Typically, the person who commits the error differs from the one who suffers the resulting damage. However, there are instances where the wrongdoer and the affected person are the same. In such cases, where a person's mistake harms themselves personally, there is no obligation for compensation from another party. Instead, the individual responsible for the error bears the burden of the damage they caused.

Under the framework of the bank's civil liability, if the bank's error stems from the customer's mistake, where the bank's wrongful action wouldn't have occurred if the customer hadn't acted erroneously, then the bank's responsibility shifts to the customer who caused the harmful outcome through their actions. An example of this scenario could be seen in a situation where a bank is considering granting a loan to a customer. Negotiations take place to determine terms such as collateral, interest rates, and others before finalizing the loan agreement. However, the bank, upon acceptance, finds certain documents missing from the customer's file, which the customer failed to provide in a timely manner. As a result, the bank discontinues dealings with the customer, leading to an interruption in negotiations. In this case, the customer's mistake

[282] Aljawarneh, S. A. *Online Banking Security Measures and Data Protection*. IGI Global, 2017.p. 22. https://doi.org/10.4018/978-1-5225-0864-9

[283] S. Oleownik, *Law and Technology in a Global Digital Society*, 2022 Springer, Phishing in Online Banking - An Overview of the Development and the European and German Legal Positions, May 2022. p.12.

becomes intertwined with the bank's mistake, as the bank's error was what ultimately caused the interruption in negotiations 7. [284] For the bank, establishing a causal relationship is the third condition that must be satisfied for its civil liability. The customer must demonstrate this link because merely proving the bank's error isn't sufficient; there must be evidence of a direct causal connection between the error and the resulting damage. The burden of proof falls on the aggrieved party, who must furnish all the elements to substantiate their claim. This entails providing evidence and supporting documentation. The bank, on the other hand, can contest the causal relationship, thereby refuting its civil liability. The acknowledgment of the bank's unified responsibility stems from the fact that the bank acts as a producer, with its services being akin to products. Consequently, we assert that the bank's civil responsibility is unified, akin to the responsibility of other producers. Given the bank's professionalism, the specific elements of its professional capacity are deemed fundamental. The bank's responsibility is tied to its existence and non-existence, leading to the characterization of the bank's responsibility as professional, akin to that of a doctor or lawyer.[285]

The fundamental principle governing the bank's obligation in electronic banking transactions dictates that the bank cannot reject or unduly delay the execution of transaction orders issued to it. Any unwarranted delay or refusal exposes the bank to liability towards the aggrieved party, who may seek enforcement through a court decision. It is therefore imperative to delineate the scenarios in which the bank's liability arises during the execution of electronic transaction orders. Firstly, if the bank refuses to execute or delays the implementation of an electronic banking transaction order as per the contract concluded between the bank and its customer, the responsibility falls on the bank. The customer commits to managing the account and accepting the implementation of payment orders and electronic banking transactions. If the bank rejects a valid order, it is liable to compensate the customer. However, the bank can absolve itself of responsibility by demonstrating that its refusal to execute the order is based on legal or contractual grounds. For instance, if the bank refrains from executing the order due to insufficient funds, it is not liable. Yet, if the beneficiary of the order accepts partial payment equivalent to the available balance in the customer's account, the bank is obligated to execute

[284] Alwa Abdel Haq, *Civil Liability of the Bank for Banking Errors towards the Customer*, Faculty of Law and Political Sciences, Larbi Ben M'hidi University, Oum El Bouaghi, Algeria, 2021. p. 323.
[285] Ibid, p. 329.

the order. The bank is not at liberty to choose whether to execute the order; it is duty-bound to do so. The order to transact establishes a personal right for the beneficiary against the bank, empowering them to compel execution if the bank refrains from voluntary compliance. [286]

The electronic transactions system defines electronic transactions as any transactions or procedures concluded or carried out, wholly or partially, by electronic means. This definition encompasses any exchange of data through electronic devices, rendering any resulting actions electronic in nature. Furthermore, the system defines electronic contracts as any agreements concluded, wholly or partially, through electronic means, thereby encompassing all actions and contracts conducted via the Internet. This comprehensive definition aims to encompass and address the evolving landscape of actions conducted via the Internet and electronic means, reflecting the system's efforts to adapt to and manage these ongoing developments.[287]

In contrast, the Saudi Electronic Transactions Law defines any act preceding or accompanying a contract's conclusion, including negotiations, as part of the electronic contract if conducted, wholly or partially, through electronic means. This law provides precise definitions for electronic contracts, data exchange, and electronic transactions to avoid confusion between contract formation and data exchange. While data exchange can occur without contract conclusion, the law ensures clarity by differentiating between the two concepts. Article 10/1 of the Saudi Electronic Transactions Law [288] holds banks responsible under tort liability if they fail to fulfill a transaction promptly, resulting in harm to the beneficiary, which constitutes negligent error warranting compensation for damages inflicted [289]. Secondly, regarding errors in executing orders within electronic banking, banks are expected to fulfill these orders accurately and in good faith as per the terms of the agreement with their customers. Any deviation from this agreement constitutes an error and holds the bank liable for civil damages to the affected customer or third parties. However, the Jordanian Electronic Transactions Law lacks specific provisions addressing this issue, leaving resolution of conflicts between electronic banks and customers to the discretion of the Central Bank of Jordan. This oversight highlights

[286] Aziz, Al-Ukaili, *The expiration of the fixed obligation in the check: a study in comparative legislation and the Unified Geneva Conventions*, D. I., Amman, International Scientific House and Dar Al-Thaqafa for Publishing and Distribution, 2001. p. 357.
[287] Act 2, Jordanian Electronic Transactions Law No. 15 of 2015.
[288] Article (10/1) of the Saudi Transactions System.
[289] Muhammad Omar, *Dhawaba Bank Transfer Contract* - A Legal Study, Master's Thesis, 1st Edition, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2006. p. 193.

shortcomings in the regulatory framework governing electronic banking operations in Jordan. It's imperative for the Jordanian legislature to address these deficiencies to create a conducive environment for electronic banking operations while safeguarding the interests of both customers and electronic banks.

Among the common mistakes made by electronic banks that violate customer instructions are errors in transaction amounts and errors in the recipient account. The bank's liability in these cases is determined as follows, error in the transaction amount, it's possible for the bank to err in executing a transaction order by transferring an amount different from what was specified. There are two scenarios to consider:

Firstly, if the bank objects due to insufficient balance during transaction execution, it has two options: either execute a partial transfer within the available balance or halt execution and inform the customer of the balance insufficiency, prompting them to replenish their account. If the bank fails to act, the customer may face claims from the beneficiary for compensation due to non-payment or delayed execution. However, if a copy of the transaction order is directly delivered to the beneficiary as a negotiable instrument, they may request partial payment within the available balance without objection from the bank.

Secondly, if an amount greater than specified in the transaction order is transferred, it could be due to either a material error or a technical glitch in the electronic banking system. In such cases, the bank rectifies the error by reversing the entry on the beneficiary's account. If the beneficiary withdraws the incorrectly credited amount, the bank may request its return, regardless of whether the beneficiary is a creditor or not.

However, complications arise when the beneficiary's account is held with a different bank. In such instances, the stage of transaction execution becomes crucial. If the ordering bank executes the transaction, it cannot unilaterally reverse the transaction but must instead seek recovery through the beneficiary. The beneficiary, however, may counterclaim against the bank by demonstrating its professional error and utilizing the general power of attorney included in the account opening contract.[290]

[290]Karaa Hafida, *electronic banking work and the civil liability of the bank therein, Faculty of Law and Political Sciences*, University of Batna, Algeria. 2019-202, p.23

III.5. Cyber Insurance For Electronic Banks

As technology advances, so do the threats posed by cyberattacks. Cybercrime has evolved from isolated hackers to organized crime syndicates with larger targets. Today, it has become a highly profitable industry, with global damages expected to double in the coming years. To access these lucrative funds, hackers are progressively using sophisticated technology such as artificial intelligence, machine learning, and automation. The use of bots and automation tools has lowered the entry barrier into cybercrime, making it accessible even to teenagers. Moreover, the emergence of tools like the new chatbot (Chat Gpt) further facilitates cybercrime activities.

Will large companies and their cybersecurity divisions remain passive in response to these challenges? Furthermore, will the rise of cyber banks fuel further expansion in the cyber insurance market, prompting subsequent inquiries into regulatory frameworks aimed at mitigating risks in this sector? Specialized institutions have reported a consistent rise in the size of the defense cybersecurity market, with expectations for continued rapid growth in the years ahead. Many countries and major companies are intensifying their efforts to bolster defensive cybersecurity capabilities to safeguard crucial data and systems. This is what is worth noting in one of the most important hypotheses on which this research is based, which is the existence of an inverse relationship between assessing the potential systemic risks associated with electronic banks and developing risk management procedures to ensure financial stability in light of the growth of the cyber insurance market, and regulation to reduce risks.

Currently valued at over $200 billion, the cybersecurity market is projected to see substantial increases in the future due to the escalating frequency and complexity of cyberattacks and crimes. In 2022 alone, cryptocurrency theft amounted to at least $3 billion, prompting significant investments in cybersecurity by major nations. Additionally, substantial research and development efforts are underway in artificial intelligence to create new cost-effective and versatile applications for both civilian and military purposes.

Electronic risk insurance, a relatively new form of coverage, serves to safeguard businesses or individuals engaged in online activities, as well as regular internet users, from risks associated with internet usage. It encompasses protection against threats to IT infrastructure and related activities. While technically falling under liability insurance, it typically requires a separate policy due to its specialized nature. Key coverage areas include theft, loss, or damage to personal

or business data, as well as disruptions to communication channels like websites, potentially resulting in financial losses through hacking. However, offering insurance for internet-connected products poses challenges due to the novelty of such risks and limited understanding of potential economic and personal harm. This type of insurance necessitates robust data and statistics to determine pricing, with emerging areas like autonomous vehicles and internet-connected medical devices presenting growing needs for such coverage.

Experts anticipate that efforts to establish a robust insurance industry in this area will yield initial results early this year. Several groups have already started collaborating on setting standards to bolster cybersecurity for internet-connected devices. It is hoped that these efforts will lead to the establishment of insurance practice standards and legal frameworks for data handling, aiding in determining liability for losses due to errors. British insurance firm engineering insurance has developed an insurance policy covering electronic piracy and associated risks, including downtime and reputational crises, targeting businesses with turnovers of less than $15 million USD, as well as medium-sized enterprises with turnovers below $75 million USD. Global economic losses from cybercrime were estimated at around $3 trillion in 2015, a figure expected to double in the years ahead.

In the realm of cybersecurity, it is an established fact that breaches are bound to happen. These breaches occur with increasing frequency and severity over time, which is an unavoidable consequence in an industry that incurs a global cost of approximately $8.4 trillion in 2022. Despite efforts to deter hackers, they persistently develop new methods to carry out their cybercrimes. During the pandemic, cyberattacks surged as the widespread adoption of connected devices became crucial for work, education, and healthcare. Despite this ongoing threat, safety measures are falling behind, posing a significant cost to the global economy. Estimates suggest that these attacks could escalate from $8.44 trillion in 2022 to $23.84 trillion by 2027. According to the World Economic Forum's State of the Connected World 2023 report, only 4% of experts worldwide feel "confident" about the security of networked devices. At the Davos 2023 annual meeting, 91% of business leaders and cyber professionals predicted the likelihood of a large-scale catastrophic cybersecurity event within the next two years. This prediction stems from geopolitical instability arising from conflicts like the Russian-Ukrainian

war and trade disputes between the US and China, drawing from past century events, breakthroughs, and security disasters.

In 2022, a multitude of major cyberattacks took place, each with distinct goals. Significantly, the Russian government coordinated breaches specifically targeting Ukraine, while there was a notable increase in ransomware assaults against hospitals and colleges in the United States. These attacks even targeted government agencies in other nations. In addition, prominent technological corporations including Microsoft, Nvidia, Uber, and Rockstar Games had massive breaches, leading to large financial and data losses. In April 2022, the Costa Rican government proclaimed a state of emergency due to ransomware attacks that caused significant disruptions to vital government operations and services. These assaults caused extensive disorder and bewilderment, affecting tax payments, healthcare systems, international trade, and compelling impacted organizations to rely on conventional pen-and-paper approaches to sustain their operations.[291] In February 2022, a hacker group named LAPSUS claimed to have successfully hacked into NVIDIA's servers, stealing about 1TB of company data, including the data of more than 70,000 employees. The company demanded the removal of a feature in its graphics cards that reduces cryptocurrency mining, and threatened to leak the stolen data if the company did not meet its demands. [292]

Finally, the implementation of monetary policies of central banks has significant effects on the market, but the economy of modern countries today is mixed, This implies that market mechanisms are dominant. There exists a market economy in modern states, where market mechanisms are dominant. However, the state still exerts influence and regulation over market conditions. This means that no individual or organization has sole responsibility for solving economic problems. Instead, economic activities are coordinated by the market without any central control.

[291] The 2022 Official Cybercrime Report highlights that the government's decision to declare a state of emergency in response to this hack is unprecedented, marking the first instance of a government taking such action in response to a cyberattack. The assault was executed by the "Conti" criminal syndicate, which is associated with Russia (it is thought to be overseen by a consortium of Russian hackers and has openly expressed its allegiance to the Russian government). The syndicate is notorious for specifically targeting victims with ransomware infections. The criminal gang demanded a payment of 20 million Dollars from the Costa Rican government in return for data retrieval. However, the government declined to make the payment and instead proclaimed a state of emergency and initiated a battle against the gang. For further information, please refer to the article titled "How the Conti ransomware group severely impacted Costa Rica and subsequently disintegrated."

[292] Global Cybersecurity Outlook 2023.

The main role of the Central Bank is to maintain the stability represented (inflation, exchange rate, interest rates) in an appropriate manner to be consistent with local economic developments and developments in global financial markets[293]. Another responsibility is to maintain stability by regulating the liquidity flow in line with financing economic activities. The significance of this stability lies in creating a conducive environment for investment, fostering high economic growth rates[294], and generating more job opportunities.

The challenges faced by Jordanian banks due to the turbulent political situation in neighboring countries and the region have been identified. There is a strong and negative impact of political turmoil on the overall flows of foreign direct investment in the region. Based on the general strategy and objectives of the Central Bank, which include assessing the risks faced by electronic banks, identifying threats to electronic information assets, and evaluating weaknesses and their likelihood of occurrence, it is crucial to meet legislative, legal, regulatory, and contractual requirements. Moreover, the principle of Cost-Benefit Analysis [295] is employed to compare the benefit of implementing controls and securing resources with the potential damage to the electronic bank's business.

As a result, the emergence of electronic banks has contributed to the growth of the cyber insurance market. It is imperative to seriously consider how to regulate this sector to reduce risks. Specialized institutions have reported a steady increase in the size of the defense cybersecurity market, and this growth is expected to continue in the coming years.

Recognizing this, the European Commission has taken proactive steps to address the increased digitization and flexibility in public administration and financial transactions. They have implemented special measures within the European Union, focusing on legal procedures and regulations, including legislation aimed at enhancing operational flexibility in the digital financial sector. The global economic crisis triggered by the pandemic has exacerbated risks due

[293] Central bank of Jordan law, no. 23 of 1971, & Mustafa,A. (2000). monetary policy and economic growth. Jordanian banks journal, vol. 19, no. 5, p. 9. (3) touqan, umaya. (2001). monetary policy aims to preserve monetary stability. Jordanian banks journal, vol. 20, no. 8, October 2001, pp. 26-27.

[294] Central bank of Jordan, financial and banking system in Jordan (1964-2004). research department. Amman: October 3 publishing.

[295] The cost-benefit analysis encompasses all pertinent benefit streams, even those for which precise quantitative figures may only be determined with a significant level of uncertainty. The process entails a comprehensive economic examination, taking into account limitations, uncertainties, market inefficiencies, and impractical scenarios. Cost-effectiveness analysis is seen as a subset of cost-benefit analysis in this context.

to reduced discipline and rapid transitions. This has led to a rise in fraud and cyberattacks, prompting central banks to realize the need for continuous policy development and electronic regulation to protect against potential threats.

An example of effective monetary policy operation during the recent economic crisis is demonstrated by the European Central Bank's implementation of a new tool—accepting corporate credit claims as collateral. This tool proved to be crucial in the euro area's monetary policy, even beyond the crisis. Additionally, the Hungarian Central Bank expanded the range of qualified collateral to include corporate loans, enabling investment funds to borrow from the central bank to cover units, thus increasing liquidity in the market.

Electronic financial operations are decentralized, allowing transactions to occur directly between customers through cyberspace without the need for financial intermediaries. While this offers advantages such as cost reduction and streamlined agreements, it also presents challenges, particularly regarding monetary regulation, money laundering, and financial consumer protection.

At the level of the legal framework and regulatory practices, the Central Bank of Jordan has worked to make necessary changes to support the use of modern financial technology and electronic transactions. These efforts aim to enhance banks' ability to manage risks resulting from financial technology (Fintech) and cyber risks, ensuring enhanced financial stability. Additionally, the activation of the electronic central system, established in 2014 as part of the Central Bank's strategic plan for 2016-2024, aims to connect affiliated banks and gradually pave the way for digital financial services in Jordan.

While the establishment of the regulatory laboratory by the Central Bank is a step in the right direction, it may not be sufficient to open the door for electronic banks. There is a need for specialized legal regulations addressing the challenges facing electronic banks and the conditions for their licensing. Currently, the door remains open for the establishment of new electronic banks in Jordan.

As a result, **Second Sub-Hypothesis**; regulators face greater difficulties in protecting the security of customer accounts and assessing the potential systemic risks associated with electronic banks, in light of the question of the responsibility of electronic banks towards

customers as a powerful and dominant party, regarding the bank's responsibility, establishing a causal relationship is a crucial condition that must be met. The customer must prove this link, recognizing the unified responsibility of the bank as a producer of services. The bank's civil responsibility is akin to that of other producers, and its professional capacity is considered fundamental. Therefore, the bank's responsibility is professional, similar to that of a doctor or lawyer, with its specific element’s integral to its existence and non-existence. Moreover, Safety and trust are crucial factors in the electronic banking sector, encouraging customers to join electronic banks without hesitation. As the dominant party in the contract, electronic banks bear significant responsibilities towards their customers. However, the absence of tangible references for electronic banks may cause hesitation among potential customers. Supervisory policies are essential for protecting customers from a legal and organizational standpoint.

Answer to the **fourth sub-hypothesis**; Regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyber attacks that could disrupt the financial system. The answer will be through whether the implementation timeline for the operational resilience framework aligns with the requirements of European legislation for operational resilience, to address operational failures and comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as cyber attacks that can disrupt the system. Financial. It defines policies, procedures and governance structures to enable us to monitor and manage the resilience of business services that matter to customers. Furthermore, as described herein Chapter III, the Cyber Incident Response Unit for the Financial and Banking Sector, this program created within the Central Bank of Jordan aims to strengthen the cybersecurity system for the financial and banking sector. It seeks to enhance the sector's readiness and ability to confront and respond to cyber risks. However, although these initiatives deserve praise, the question remains: Are they sufficient to pave the way for the establishment of electronic banks in Jordan, it is worth noting why the Central Bank has not implemented specific legal regulations to address the challenges facing electronic banks and determine the conditions for their licensing. These systems would play a pivotal role in opening the door to the establishment of new electronic banks in Jordan. By doing so, Jordan can take an important step forward in attracting external liquidity and promoting large-scale investments from large companies in the electronic banking sector.

Chapter IV

The Legal Situation Of Revolut Bank - Case Study

This chapter will discuss the most significant international experiences in electronic banking, analyzing them in terms of documented reports issued by electronic banks and their compliance with international banking laws. It will focus on proposing a legal model for implementing the experience of electronic banks in Jordan. This model will be designed to achieve financial security amidst the growing concerns surrounding challenges facing the legal regulation of electronic banks.

In this segment of the chapter, we delve into an analysis of Revolut Bank as case research within the EU, researcher aim is to extract insights that examining the legal procedures adhered to during its expansion, the risks encountered, customer protection frameworks, and future trajectories. Additionally, seeking to align the experiences of selected the bank with both international governing laws and national and local regulations. Ultimately, my goal is to construct a model for electronic banking in Jordan that not only draws from international experiences but also conforms to local legal standards and international norms. Additionally, Examination of Revolut Bank, a prominent electronic bank in the European Union monitored by the European Commission, draws upon a comprehensive review of the bank's website [296] and an analysis of its issued reports. Through this process, scrutinize the intricate details of Revolut Bank's operations to glean valuable insights into the functioning of electronic banks within the European Union and their alignment with legal regulation frameworks.

On the other hand, examination, will reference the EBA Digital Platforms Report for September 2021, The European Banking Authority (EBA) performed a comprehensive evaluation of

[296] Access on 7 Feb 2023: https://www.revolut.com.

market trends, which including an examination of the involvement of major technology firms in the banking and payments sector of the EU. This research serves as the foundation for creating a strong model for electronic banking in Jordan, customized to address the country's unique requirements while following worldwide standards and regulations.

In fact, the researcher had many motives for studying Revolut Bank in this research, the most important of which is that Revolut, being a completely digital and cloud-based bank, was able to work well during the Covid-19 pandemic and its repercussions. Employees were able to work remotely without any major interruption. Stringent measures have been taken to closely monitor cyber threats associated with the remote working model, the innovative and expanding digital organisation, and the ongoing opportunism and motivations of criminals. These procedures include implementing additional controls to ensure the safety of customers, employees, and data. It is also considered one of the largest and most important electronic banks in the EU.

In addition, Revolut has a proactive strategy to enhance security measures, adapting to changes in the threat environment through continuous testing and auditing processes. Revolut will work to develop its governance in this area and aims to comply with external information security standards, such as SOC2, to ensure the reliability of Revolut control system for consumers, partners and suppliers who use Revolut services[297]. This was the primary motivation for the researcher to adopt the Revolut Bank experience as a "case study" to be taken. Including lessons and lessons, and to be an approach that will be enlightened and guided in Jordan in the future to achieve the legislative agenda in the electronic banking sector; it is worth noting and emphasizing from what was previously mentioned one of the most important **hypotheses** on which this research was based and built, which states that Regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system.

Revolut, established in the UK in 2015, provides remittance and foreign exchange services that are quicker and more cost-effective than those offered by conventional banks. As of November 2022, Revolut has amassed over 25 million retail clients in more than 35 countries worldwide. The annual report and consolidated financial statements for the year 2021 include crucial information about Revolut Ltd (registered number: 08804411). It is a recent addition to the

[297] Revolut Ltd, Annual Report And Consolidated Financial Statements, For The Year Ended 31 December 2021.

electronic banking sector that has experienced increased popularity during and following the Corona crisis. The key founders of Revolut Bank are Martin Gilbert, who serves as the President, and the bank is established, the bank's registered office is located at 7 Westfire Circus, Canary Wharf, London.

I will endeavor in this chapter to examine the main hypothesis and its associated sub-hypotheses in the context of analyzing international reports on financial transactions, governing laws, and existing electronic banking cases; By examining the experience of Revolut Bank and scrutinizing its operations as a prominent electronic bank recognized globally by various official and legal entities, i aim to address the hypotheses of the research by drawing insights from the Revolut Bank model and the report issued by the European Commission on February 2021, there was a discussion on digital money and the associated regulatory problems. This include the oversight and control of fragmented or non-integrated sequences of operations that involve the provision of financial services, as well as the management of risks connected with companies that combine multiple activities. These responsibilities are detailed in the European Commission ESA 2022.01 study. In addition, we will take into account both international regulations and the Jordanian Legislative Law on Electronic Financial Transactions.

IV.1. Financial Performance of Bank

The bank's growth trajectory remains on an upward trajectory, coupled with significant profitability. Revenue almost tripled in 2021, leading to a £59.1 million profit from operations. This robust financial performance underscores Revolut evolution from a growth-focused "startup" to a profit-driven "expansion" phase. In July 2021, the company secured US$800 million through Series E funding, valuing the business at US$33 billion. In 2021, banking services were introduced in 18 European countries, further expanding the bank's presence in the United States. Our app caters to the modern American consumer's needs at a competitive price point, offering features such as US/Mexico transfers and fee-free services for ATM withdrawals, international transfers, and cryptocurrency trading. In September 2021, approval was granted for the broker's license application in the United States. Additionally, in January 2022, the

commission-free stock trading platform was launched in the United States, boasting over 1.1 million users.

IV.2. Spread And Scope Expansion Revolut Bank

Revolut Bank's financial information is disclosed in accordance with the International Financial Reporting Standards (IFRS). As of the start of 2021, Revolut Bank has a client base of 11 million. In spite of the limitations imposed by COVID-19 on travel and social media, the number of retail customers increased by five million (equivalent to an average of over 15,000 each day), along with the addition of several commercial customers. By 2022, the number of retail customers had reached 25 million.[298]

Revolut has allocated additional resources to enhance fraud detection and prevention measures, as well as to educate our clients on effective strategies to safeguard themselves against various types of fraud, in compliance with regulatory standards and industry best practices. Revolut has implemented advanced measures to detect and prevent client abuse by fraudsters. These measures include the use of powerful machine learning models and engaging with customers to counteract fraudulent conduct. Additionally, Revolut relies on product innovation to enhance its fraud prevention capabilities; the above brings us back to the question and to one of the parts of the **research question**, which is the third sub-question: What are the regulatory challenges and risks facing independent e-banks and their protection.

In 2021, there were several significant accomplishments and advancements. The Financial Market Supervisory Commission of the Bank of Lithuania has granted the MiFID license application, allowing the Bank to offer trading services to all clients in the European Economic Area (EEA) and extend its worldwide presence.

Revolut Bank expanded its operations to Lithuania and Poland in 2020, bringing the total number of countries in the European Economic Area (EEA) where it operates to 18. By the end

[298] The bank's profitability came despite the economy facing a significant long-term shock due to global lockdowns, ongoing travel restrictions, and the impacts of the coronavirus. However, at the same time, "the acceleration towards digital and remote services has led to an increase in our customer base and their usage of our application." Product Innovation, in 2021.

of the year, the European Central Bank (ECB) gave Revolut Bank a full banking license, replacing its previous specialized banking license. The Bank was authorized to finalize the merger in 2022, combining our electronic money services with the Bank's enterprises to offer banking services to all our clients in the European Economic Area. Revolut Bank as well In 2022, the company expanded its lending operations in Lithuania and Poland by introducing them in Ireland and Romania.

The acquisition of trading licenses in Australia and Singapore was completed, and trading services were introduced in Australia in February 2022, followed by their introduction in Singapore later in the same year. The Financial Industry Regulatory Authority (FINRA) approved their broker-dealer license in September 2021, allowing them to provide trading services to clients in the United States starting from January 2022. A novel social trading tool has been introduced in the United Kingdom, allowing consumers to get insight into the investment choices of leading traders. Trading clients may leverage the social trading function to get knowledge from proficient stock traders and exchange investment methods with fellow traders. In 2021, the investment in cryptocurrencies shifted from being limited to early adopters to being more popular among mainstream investors. This change was fueled by the growing interest and involvement in cryptocurrencies among financial media, markets, and financial institutions. The quantity of tradeable tokens available has expanded from 10 to 60, offering customers the chance to invest in a wide variety of cryptocurrency tokens. In order to achieve the bank's goal of becoming a highly esteemed worldwide financial institution, it is imperative to pursue global expansion. In 2019, we took the first steps to broaden our services by extending them to Australia and Singapore. The growth initiative commenced in 2020 with the development of expansion centers in the United States and Japan. With a strong emphasis on the U.S. market, we prioritize it as a major strategic focus and a market with significant growth potential. Notwithstanding these obstacles, the bank achieved substantial advancements in expanding our clientele in the United States, in the second quarter of 2021, it successfully expanded its range of products and acquired a broker-dealer license from FINRA. This license allows for the introduction of stock trading in the US.

In 2021, preparations were made for the introduction of Revolut in Latin America. Revolut found Latin America to be a highly appealing market due to the rising usage of digital payments, the intricate nature of regional foreign exchange markets, and the increasing popularity of

cryptocurrencies and their limited supply. Brazil and Mexico have become prominent markets in the area due to their strong compatibility with our existing geographical presence. During the year, the bank established Revolut Technologies Brazil LTDA and Revolut de Mexico S.A. de C.V., forming teams in both countries under the leadership of Glober Mota (CEO for Brazil) and Juan Miguel Guerra (CEO for Mexico).

Table No. (**2**) shows the committees organizing the work in particular at Revolut Bank and how to sequence duties and manage risks and reduce them, until threats are controlled.[299]

Principal	**Risk Mitigants and Controls**	**Outlook**
Regulatory Risk		
Revolut is dedicated to adhering to the applicable regulatory obligations in the regions where it conducts business and to delivering precise, dependable, and prompt reporting to external stakeholders, authorities, and regulators.	Revolut manages and reduces the potential negative impact of regulatory factors by implementing its Enterprise Risk Management Framework. Comprehensive rules and processes, supported by a thorough obligatory training program, increase regulatory risk management. The exercise of governance is carried out by the Compliance, Operational & Conduct Risk Committee, which has well-defined channels of escalation to the Group Executive Risk Committee and the Board Risk & Compliance Committee. Revolut has a robust Horizon Scanning approach to promptly identify initial indications of significant regulatory, legislative, and policy advancements or modifications. Revolut regularly participates in and offers insights on consultation papers produced by regulators.	Revolut aims to comply with all applicable rules and regulations and build robust partnerships with regulators. Comprehending regulatory standards may be intricate and necessitate meticulous interpretation, which involves taking into account their fundamental essence and purpose. We are dedicated to adhering to relevant laws, rules, and regulations and actively monitoring any changes in the regulatory environment. We will also ensure the maintenance of strong systems and controls.

[299] access on 7 Feb 2023 ; https://www.revolut.com

Principal	Risk Mitigants and Controls	Outlook
External Fraud Risk		
External Fraud risk, as defined by Revolut, refers to financial damages resulting from deliberate activities aimed at deceiving, unlawfully taking possession of property, or evading legal regulations, committed by a third party. Revolut has notable external fraud risks, which encompass acquiring fraud, as well as issuing fraud related to cards, payments, and lending. Account Takeover Fraud and Application Fraud, sometimes known as Identity Fraud, are types of fraudulent activities. Revolut has a minimal tolerance for External Fraud Risk. Revolut specifically prioritizes mitigating the risk of users falling prey to Account Takeover Fraud, Authorised Push Payments Fraud, and lost or stolen Card Fraud. Revolut is dedicated to adhering to the applicable regulatory standards and recommendations. Moreover, any failure to comply may result in enforcement measures, such as monetary penalties.	Revolut strives to minimize the risk of external fraud by implementing strong and effective systems and controls. These measures are meant to comply with current laws and regulations, as well as to discourage, prevent, detect, manage, and report instances of external fraud. Revolut conducts comprehensive investigations into instances of fraud to acquire information and make necessary actions to improve its systems and procedures. This measure is being implemented in order to protect Revolut and its clients from any fraudulent activities and maintain the company's reputation. In addition, the group is mitigating the most significant risks by enforcing mandatory training for all employees and employing specialist Key Risk Indicators (KRIs) to identify patterns in fraudulent instances.	Revolut strives to minimize the risk of external fraud by implementing strong and effective systems and controls. These measures are meant to comply with current laws and regulations, as well as to discourage, prevent, detect, manage, and report instances of external fraud. Revolut consistently assesses, monitors, and enhances the efficiency of its External Fraud Framework. The company is dedicated to upholding a risk and control environment that allows it to rapidly and efficiently address any new fraud risks and sophisticated technologies.
Third Party		
Risk Revolut depends on other entities and contracted service providers for various operations, such as payment processing, adherence to regulatory requirements, foreign and cryptocurrency exchange, trading services, KYC/AML procedures, and other business-related services. A substantial proportion of the services offered to Revolut clients rely on third-party agreements. As a result, this creates both operational and concentration risk, which we have a clearly defined tolerance for and	The Group manages this risk by implementing a comprehensive strategy for managing third-party and outsourcing risks. This include the continuous monitoring of outsourced services, Service Level Agreements, and the implementation of contingency planning measures. Collaborating closely with other entities to guarantee our ability to withstand challenges and maintain uninterrupted delivery of our services. We	The expansion of our business has led to an increase in the number of third parties in our network. We are actively monitoring this risk. As a regulated institution, we conduct regular reviews of our systems and processes. Our third-party due diligence methodology has undergone significant changes in 2021 and will continue to evolve in the future.

Principal	Risk Mitigants and Controls	Outlook
monitoring processes in place. In addition, some of our third-party partners depend on a significant workforce that requires specialized training to effectively support our services.	aim to decrease our reliance on external entities by diversifying and developing our own goods and processes internally, if feasible.	
Availability & Continuity Risk		
Operational Resilience is an outcome which Revolut strives to achieve by effectively managing its Availability and Continuity Risk and responding to operational disruptions in a timely manner. Operational disruptions can have many causes including, for example, technology failures or when making changes to systems. Some disruptions may also be caused by matters outside of a firm's control, such as a cyber-attack or wider telecommunications or power failure. Operational disruptions always remain a risk, As Revolut expands its operations, introduces new products, and enters new areas, the probability of experiencing operational disruptions is expected to rise. With the expansion of the consumer base, the possible consequences are likely to escalate. Ensuring operational resilience is crucial for Revolut to safeguard its clients and accomplish its growth objectives.	The Group has established an Operational Resilience Framework which sets out the policy, procedures and governance structures to enable us to monitor and manage the resiliency of our most Important Business Services for customers. The Operational Resilience Framework is formed of nine capability pillars which cover a variety of potential sources of operational disruption and support us in defining 'resilience practices' under each pillar. Revolut maintains a suite of Business Continuity Plans and Disaster Recovery Plans which contain recovery measures for business processes and technology to enable services to be resumed.	Revolut Operational Resilience Framework has identified our most Important Business Services for customers, and set tolerance limits for their disruption in a major incident will continually work to enhance the resiliency of these important services, by investing in additional technology, people and third-party resources. The aim of this is to limit the likelihood of a major disruption occurring, and also to limit the harm to customers and Revolut should a disruption impact the Group, and establishing a robust testing regime to monitor the effectiveness of our resiliency measures across the Group.

Source (table no. 2); Revolut Ltd, Annual Report And Consolidated Financial Statements, For The Year Ended 31 December 2021.

Revolut bank is committed to diligently preventing and detecting financial crime. Revolut addresses these risks by implementing a strong governance structure, efficient risk management procedures, and a solid control framework to handle Financial Crime Risk. Additionally, Revolut continuously enhances the effectiveness of its financial crime systems and controls

through real-time transaction monitoring, daily screening of all customers for sanctions and negative media, and comprehensive mandatory training for staff on Financial Crime Risk. Revolut remains committed to investing substantial effort and resources to bolster the overall financial crime framework, systems, and controls.; It is worth noting and emphasizing from the above mentioned the most important two **hypotheses** on which this research was based and built, which state that Regulators face greater difficulties in protecting the security of customer accounts and assessing the potential systemic risks associated with electronic banks, in light of the question of the responsibility of electronic banks towards customers as a powerful and dominant party. As for the second hypothesis, which was emphasized by Revolut Bank previously, Additional qualification requirements are needed for employees working in electronic banks related to preventing involvement amid accelerating threats such as money laundering.

In fact, electronic banks are in their early stages of development and may not have established the same degree of trust as traditional banks. Customers may exhibit hesitancy in placing faith in a bank that lacks a physical presence, and they may harbor apprehensions over the security of their online transactions. Nevertheless, several e-banks are covered by the Federal Deposit Insurance Corporation, providing consumers with a sense of reassurance, fostering confidence, and establishing a positive reputation. A multitude of electronic banks provide exceptional customer care and user-friendly applications or websites. Additionally, it may provide distinctive attributes like high-yield savings accounts or no-fee checking accounts in order to attract consumers. The prominence and recognition of e-banks is anticipated to increase as they gain more popularity and become more prevalent. [300]

[300] Al-Atrash, Heba, and Muhammad Belhassan. "Factors Affecting the Adoption of Electronic Banking Services: A Quantitative Study of a Sample of Algerian Bank Customers." *Journal of the Institute of Economic Sciences* 24, no. 1 (2021).p.167-185.

IV.4. Engaging With Stakeholders

At the time of publishing, Revolut had over 25 million customers, 5,000 staff, and operations in 35 countries, making it a rapidly expanding firm with several influential stakeholders globally. Among them are our workers, partners, suppliers, consumers, regulators, and investors.

The success of Revolut hinges on its ability to establish and maintain positive relationships with its stakeholders. The Board acknowledges its duty, as outlined in Section 172(1) of the Companies Act 2006, to promote the company's long-term success while considering the various stakeholders in making business decisions.

In order to address long-standing issues, Revolut has created innovative technologies. Launched in 2021, the Delivery WOW initiative aims to give clients memorable and good contacts during times of need.[301] Recruit a fresh group of customer experience managers to monitor social media and all other channels for client input. Consistently improving the customer journey, working closely with the product and service teams to prioritize future improvements and developments, establishing trust between electronic banks and customers, and promptly responding to customer reports of financial fraud are all part of their job.

IV.5. Fraud Prevention And Customer Safety

There is no sector of business or society that is immune to the negative effects of fraud, which is a worldwide problem. Revolut has made significant investments in 2021 to safeguard users from fraud using a mix of cutting-edge machine learning methods, in-app notifications, and client education campaigns: For instance, Revolut ran anti-fraud campaigns to have its name included in a law that would have made it easier for financial institutions to exchange intelligence and ensure the security of customers' personal information while transacting online; These actions taken by Revolut Bank indicate and confirm one of the **hypotheses** on which this research is based, which states that Regulators need to develop comprehensive crisis

[301] Revolut, a global financial technology company, emphasizes a core value known as "Deliver WOW." This principle reflects their commitment to exceeding customer expectations by providing exceptional service and innovative solutions

management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system.

Joining together with politicians and government authorities, Revolut's top management brainstormed ways to tackle the fraud problem by investing in staff and machine learning technology. Attended the Strategic Council for Economic Crime, the premier platform to address economic crime, where Revolut's Head of Risk Management, Pierre, shared the company's knowledge with the United States, the United Kingdom, and their respective secretaries of the treasuries and ministries of interior. Additionally, to the Money Laundering Intelligence Task Force, an alliance of the banking industry and law enforcement to disseminate and evaluate data pertaining to money laundering and other economic dangers.

For optimal client outcomes and sustainable growth over the long run, it is critical for an organization's culture to place a premium on excellent governance, risk management, and transparency. To thrive in its highly regulated industry, Revolut relies on a robust Board and a positive company culture that permeates the company from the top down. There are two levels of risk on Revolut as well. Primary (L1) Financial, operational, compliance, behavior, and strategic risk make up the five basic categories of risk. Within each level and one category, there are defined danger zones at the second level (L2). It keeps all the specific hazards in each L1 and L2 category in one central library, making sure they are consistent and comprehensive. L1 (Corporate) Risks in Classification Risks to Revolut's overall business operations and the attainment of its strategic and core goals must be addressed as part of the company's strategy. Internal process failures, human mistake, system malfunctions, and external events influencing the firm are all examples of operational hazards. There is always some operational risk for every given firm, and that risk tends to expand in proportion to the complexity and size of the enterprise. Financial assets and liabilities of the bank are vulnerable to these risks, which include capital, liquidity, market, and credit risks. Credit risk connected with client lending is one example of the financial risk that Revolut Bank acknowledges as part of its business strategy. The risk of noncompliance with applicable laws, regulations, and industry standards in the countries where Revolut does business is known as compliance risk. Conduct risks include any decisions or failures to act by Revolut or its representatives that might have a detrimental effect on stakeholders, customers, market stability, or effective competition.

During 2022, researchers increasingly worked to improve its Enterprise Risk Management Framework (ERMF)[302] to accommodate the risk management implications of the growth of online banking and increasing complexity in its structure, geographic spread, and product offerings. Many additional tools and methods have been developed as part of this framework, including the most important reason which I shall elaborate as the framework's central tenet; Revolut is implementing a uniform risk strategy, improving its identification procedures to better monitor, manage, and resolve its most significant risks, and mapping its risks across all departments. By integrating visual representations of risk and related events into the risk platform, we can improve our risk register and control, streamline our risk management process, identify and monitor areas that need increased oversight from the risk and compliance function, identify and capture highly improbable scenarios that could impact Revolut operations, document roles and responsibilities via LoD3, and integrate them into the ERMF. This allows for standardized risk clarification across the organization and aggregation of similar risks from different departments. An annual control testing process allows for seamless monitoring of policy implementation, the Three Lines of Defense Operating Model (LoD3) automates the policy adoption process, and a comprehensive policy framework was developed to address each risk. The model categorizes risks through appropriate policies and procedures, which serve as guidelines for business operations. Additionally, a platform was established to directly link policy data to the control log. All of this contributes to improved internal policy management. Level I policies are those that have been accepted by the Board of Directors, Level II are those that have been adopted by the Executive Committee, and Level III are those that have been approved by the Department of Management.

[302] Based on the risk appetite of the department and our risk environment, the Enterprise Risk Management Framework (ERMF) provides a thorough method for discovering, analyzing, and treating risk.

The table (**3**), shows how risks are managed and what risks the electronic bank Revolut Bank [303]

Risk Management Procedures At Revolut Bank	**The Risks**
Key performance indicators (KPIs) are used to monitor how well Revolut is doing in achieving its stated goals, which are in turn determined by the Board of Directors and overseen by the Executive Committee. It uses formal procedures to investigate and fix possible or actual violations, as well as other automated monitoring systems called KRIs (Key Risk Indicators), to keep an eye on threats to its strategy. The Group CEO of Revolut identifies the most critical strategic risks facing the firm. The executive team then examines and analyzes the identified risks on a regular basis. A report is then produced outlining the most critical risks, how they affect the company's objectives, and any measures taken to mitigate them. The Group CEO is updated on upcoming developments every quarter by the Risk Committee, the Board of Directors, the Compliance Committee, and the Risk Committee.	**Revolut strategy**, Critical threats are those threats that intimidateto interfere with Revolut version materially impacting the financial institution's capability to attain its tactical goals. The change of calculated dangers is most impactful as it concentrates on the following: Outside elements such as the lack of ability to recognize, analyze, as well as handle macroeconomic, governing, political, as well as social elements might prevent the application of the financial institution's approach. This consists of the capacity to determine as well as prepare for high-impact occasions. Threats emerging from our calculated options. Threats that show the financial institution's society as well as do not sustain its critical purposes, such as: Track record threats from our numerous points of view as well as stakeholder teams which might frequently develop as an additional result.

[303] Access on 7 Feb 2023: https://www.revolut.com.

	The sustainability of development campaigns which includes the threat of attaining temporary gains at the expense of long-lasting success. Functional threats might cause hold-ups in item distribution, business advancement as well as the connected threats as well as the lack of ability to adjust and also explain and dressmaker items to satisfy different market objectives.
Key Risk Indicators limit the impact of potential capital losses. This allows for quick response in the event that the group's capital situation worsens. In order to address potential risks, the group will establish capital buffers to guarantee it has sufficient capital according to its risk profile. Every year, the Internal Capital Assessment Process reevaluates the group's capital requirement. On a yearly basis, we also assess our recovery strategy. A robust process for tracking the group's capital position is in place, with quarterly reviews considering anticipated growth and the launch of new entities. The group also has a set of capital KRIs and a comprehensive recovery plan to handle situations where a capital deficit is possible, all of which help to reduce the group's exposure to major capital risk. The recovery plan framework should be used in conjunction with macroeconomic	Revolution has identified the following as the greatest capital risks: - A lack of funds, which becomes particularly problematic when facing market pressure or when seeking aid for expansion.

monitoring to ensure that appropriate measures are taken in response to changes in the macroeconomic environment.	
By monitoring its exposures with key risk indicators and appropriately identifying the sources of such risk, Revolut controls its market risk. Lessen potential harm and take advantage of hedging deals where necessary. We evaluate possible market risks in both normal and high-stakes situations. Our KPIs include commodities, cryptocurrency, and foreign exchange price and fair value tracking metrics.	The skill to acquire capital by commercial means, in a dynamic market, on equitable terms, even during economic downturns.
Procedures and controls for retail and commercial credit products are overseen by the respective Risk Committees at the group and entity levels. Accurate, trustworthy, and timely reporting to external stakeholders, authorities, and regulators is an important part of Revolut's mission, as is compliance with any regulatory obligations in the jurisdictions where the company operates.	Trade credit, retail credit, and wholesale credit all pose threats to Revolut. most people The exposure to high-quality sovereign and corporate counterparties through treasury assets, the placement of corporate funds and the protection of client funds with institutional money all contribute to wholesale credit risk. In a variety of countries, Revolut extends credit to both individuals and businesses through its retail lending portfolio, which mainly includes unsecured personal loans and credit cards, and its commercial credit exposure. Cultural risks associated with business processes and incentives, as well as behavioral risks pertaining to consumer

	outcomes, market stability, and effective competition, are concerns for Revolut. Customers are at the center of Revolut's business strategy, and the company is dedicated to satisfying them. Everything from products and services to communications and after-sale support falls under this umbrella.

Source (table no.3);Revolut Ltd , Annual Report And Consolidated Financial Statements, For The Year Ended 31 December 2021.

On the other hand, to inform examination, will cite the September 2021 EBA Digital Platforms Report, in which the European Banking Authority (EBA) evaluated market trends, including the impact of large digital firms on the financial services industry in the European Union (EU). Also considered in an effort to validate the research's central hypothesis is the European Banking Authority's (EBA) study of EU national coordinating authorities about regulated financial services operations conducted by Big-Tech Group businesses. In addition, we will examine the results of the EBA's and national competition authorities' comprehensive studies of the present preventive measures for specifications and metrology[304].

Additionally, value chains that are not cohesive or linked. The banking industry has long been dependent on outsourcing and other forms of third-party service provision. Companies in the financial and non-financial sectors have long worked with and been outsourced to by financial institutions.[305] This has long been overseen and regulated by the European Union (EU) in accordance with its standards for good governance, risk assessment, and outsourcing. Third parties within the value chain are becoming increasingly important to financial institutions as a result of technological improvements and digitalization. Indeed, as a result of the COVID-19

[304] EBA (2021e), Report on the use of digital platforms in the EU banking and payments sector, EBA/REP/ On 26 September 2021.

[305] E.g. insurance undertakings with reinsurance undertakings, investment firms with clearing and settlement services providers, banks with payment service providers and payment card schemes.

epidemic, there has been a rapid acceleration in the trend of financial institutions depending on third-party data and technology for their digital transformation. Agencies in the financial sector also take notice of encounters Fintech, large tech businesses, and established financial institutions are expanding their collaboration models to include mergers and acquisitions, joint ventures, outsourcing, and partnerships. Along with introducing new goods or services that capitalize on their complementary strengths, these firms also participate in co-innovation. The emergence of value chains that are produced, managed, and controlled by technology businesses or other third parties is prompted by the fact that certain technology suppliers interact with several financial institutions. [306]

When it comes to providing regulated financial services, financial institutions face competition from fintech and large digital businesses. Efficiency, competition, and innovation are driving these trends, even if huge internet companies still have very restricted access to regulated financial services in EU nations compared to other jurisdictions. Nevertheless, this issue deserves monitoring. In order to devote more resources to running the models and adding value, financial institutions may decide to outsource their non-core operations. Technology firms are showing that some value chain procedures can be better handled as independent services. As a matter of fact, the value chain becomes increasingly specialized as fragmentation increases. For instance, banks can save money by switching to cloud infrastructure from on-premises data centers. To provide customers with useful and affordable digital solutions, financial institutions are also utilizing the expertise of other parties. Software developers cater to the stock market by providing individualized solutions to enhance clearing, settlement, trading, and collateral management. Financial planners and insurers are increasingly utilizing AI to craft personalized investment strategies and life insurance plans for their customers.[307]

This pertains to either loan management or customer services (KYC). There is a proliferation of data-centric business models, as well as an increase in the variety of products and services available (such as crypto-on-demand, P2P and traditional insurance, smart contracts, and e-payment services). New regulatory technology solutions (RegTech) are also on the horizon; these can alleviate operational hazards, cybersecurity concerns, fraud during remote preparation, and regulatory reporting. Working together may shorten the time it takes to bring new projects

[306] EIOPA (2020b), Discussion Paper on the (RE)insurance value chain and new business models.
[307] See responses to the Call for evidence on Digital Finance on ESMA website.

to market, which in turn allows for more data availability, faster data standardization, and economies of scale. Data availability and the capacity to standardize or analyze massive volumes of data have also grown substantially, which is a driving factor in these advancements.[308]

Global data production is projected to increase from 33 zettabytes in 2018 to 181 zettabytes in 2025, according to the European Commission[309] , as well as financial sectors, anticipate a rise in the commercial use of data across the economy. In a similar vein, the variety of data at one's disposal, which may include non-financial information like behavioral data, IoT, social media, and ESG (environmental, social, and governance) data. as a result of the development of open data principles, ESG is quickly growing [310] , While third-party data does not yet fully supplant conventional datasets, it is becoming more and more used by financial institutions to determine creditworthiness and provide personalized investment recommendations. When it comes to banking, for instance, analytics are still mostly based on core banking data, not data sourced from places like social media. Reasons for this might include ethical considerations surrounding data access and usage and organizations' worries about the veracity and quality of external data. Data from emerging sources, including internet media, is supplementing (rather than replacing) older sources in the insurance industry, such as exposure data and demographics.[311], giving more frequent and detailed information on customer traits, habits, and way of life. This paves the way for better risk evaluations and more personalized goods and services. Investment choices made by asset managers in the stock market are being informed by a wider variety of data, including non-financial alternative data. As a result, the relationship between banks and other third-party data suppliers becomes more interdependent.

The utilization of cloud computing, which has become an essential component of financial services, has contributed to the exponential growth in computing power as well as the ability to store and analyze data. By facilitating the effortless integration with consumer-facing mobile applications, cloud computing speeds up data analytics and provides access to massive quantities of storage space. For instance, out of all the insurance businesses, 33% employ cloud

[308] This concerns data in general, not necessarily data relevant to financial services.
[309] IDC and Statista (2021), *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025 (in zettabytes)*, Graph, 7 June, Statista website.
[310] EBA (2020c), EBA report on Big Data and Advanced Analytics, EBA/REP/2020/01, January.
[311] EIOPA (2019b), Big Data Analytics in motor and health insurance: a Thematic Review.

computing services for car and health insurance, and another 32% want to do so during the next three years [312], The Emirates Authority for Standardization and Metrology, as reported by Statista.

Financial services can take advantage of new features made possible by some cloud providers' bespoke cloud solutions, such as enhanced client onboarding, profile and sharing identification, assessments of regulatory compliance, and data encryption, which will make previously classified personal data usable for analytics. Virtual health and wellness services, such as self-assessment and preventative tools, a remote consultation interface, and document acceptance, are made possible by digital healthcare platforms that certain insurers develop in partnership with cloud providers. online, in-home care services) or cybersecurity programs that help small and medium-sized enterprises (SMEs) become more cyber resilient and less vulnerable to cyber threats. Despite cloud computing's promise of lowering IT infrastructure costs, there remains a significant risk of concentration. [313]

in addition to the growing utilization of AI and big data. A lot of banks and other financial organizations have started digital transformation initiatives with AI at the center in order to cash in on digitalization's benefits.[314]

In particular, processing datasets is seeing a rise in the usage of generative AI systems. Both new and old, targeting specific audiences with advertising campaigns or providing customers with more personalized offerings. In 2018, a third of the European insurers who took part were already utilizing machine learning, with a further quarter in the proof-of-concept phase , and in some jurisdictions, the level of adoption was already 100%.[315]

Although many financial institutions have the resources in-house to provide big data and AI services, they generally outsource these tasks to third-party technology firms. [316] Financial institutions often employ AI systems that integrate data from both internal and external sources, such as consumers' or the institutions' own production or data given by other organizations.

[312] EBA (2020c), EBA report on Big Data and Advanced Analytics, p. 11.
[313] Scott, H., J. Gulliver, and H. Nadler. "Cloud Computing in the Financial Sector." 2019, pp. 12-14.
[314] FSB (2019a), FinTech and market structure in financial services: Market developments and potential financial stability implications, 14 February, p. 16-17.
[315] EIOPA (2019b), Big Data Analytics in motor and health insurance, p. 6.
[316] Joint Committee of the ESAs (2018), Joint Committee Report on the results of the monitoring exercise on 'automation in financial advice', JC 2018-29, 5 September, p.9.

Rating of credit, public storage facilities, or academic institutes [317]. Outside of cloud computing and artificial intelligence/machine learning, technology businesses are hired for a variety of specialized tasks. There have been advancements in areas like electronic signatures and biometrics, which are utilized for client authentication and authorization, as well as in areas like ESG research and big data and analytics.

Cryptocurrency and Open Financial Systems Indeed, open finance is just another invention that boosts retail, competition, and innovation. For a while now, people have been talking about open finance, with a primary emphasis on banks and PSD2 (open banking). New European Union policies, including data strategy by the Commission[318], and the digital finance strategy[319] understand and express the significance of data-driven innovation and data flows in the European Union The banking sector is no longer the only one that uses application programming interfaces (APIs) to exchange data, both personally identifiable and otherwise. The use of open APIs has the potential to spur innovation across sectors and make businesses more adaptable to shifting consumer preferences. Better policyholder services and/or more market competition are two goals of the open finance movement, which seeks to increase access to companies' internal A PIs through means such as the integration of financial institutions with platforms and other third parties. [320] The market environment has been significantly shaped by the PSD2 framework on the payments front. Banks and other payment service providers are required by this framework to have open banking policies that allow authorised third parties access to their customer accounts. Aiming to encourage more digitalization and competition in the payments business, PSD2 does this.

Financial crime prevention and detection is a top priority for Revolut Bank. Strong governance, efficient risk management processes, and a solid control system to handle Financial Crime Risk are ways Revolut reduces these risks. Revolut is devoting a lot of resources to bolstering the

[317] The use of big data analytics tools by insurance undertakings takes place throughout the insurance value chain, predominantly in the areas of pricing and underwriting, claims handling and sales and distribution.
[318] McKinsey assessed that opening financial data could increase EU GDP by 1-1.5% by 2030; McKinsey Global Institute (2021), Financial data unbound: The value of open data for individuals and institutions, Discussion Paper, June, p.10.
[319] See the European Commission's communication and factsheet from 19 February 2020, available at: European data strategy, EC website.
[320] The Commission announced in the DFS that it will present a legislative proposal for a new open finance framework by mid-2022, building on and in full alignment with broader data access initiatives.

overall framework, systems, and controls for financial crime. This includes real-time transaction monitoring, daily customer screening for sanctions and negative media, and improved staff mandatory training on financial crime risk.

Financial crime prevention and detection is a top priority for Revolut Bank. Strong governance, efficient risk management processes, and a solid control system to handle Financial Crime Risk are ways Revolut reduces these risks. Revolut is devoting a lot of resources to bolstering the overall framework, systems, and controls for financial crime. This includes real-time transaction monitoring, daily customer screening for sanctions and negative media, and improved staff mandatory training on financial crime risk.

As a matter of fact, people may not have as much faith in electronic banks just yet because they are still in their early stages. Customers may be wary of doing business with an online bank due to security concerns and the fact that they can't visit the branch in person. On the other hand, the Federal Deposit Insurance Corporation insures a number of online banks, which is reassuring to consumers and helps these institutions gain credibility. You may find user-friendly applications or websites and great customer service at many online banks. Unique features, such fee-free checking or high-interest savings accounts, could be offered to attract users. As e-banks gain traction, their reputation and visibility are projected to increase.[321]

[321] Al-Atrash, Heba and Belhassan, Muhammad. 2021. Factors affecting the adoption of electronic banking services: A quantitative study of a sample of Algerian bank customers. Journal of the Institute of Economic Sciences, MG. 24, p. 1, p. 167-185.

Chapter V
Results and Discussion

V.1 The Conclusions

This chapter aims to address the questions and hypotheses of the comparative descriptive manner. It will test and answer hypotheses within an organizational plan that presents topics, experiences, and results. Building upon the issues explored in previous chapters, including electronic payment, electronic documentation, potential risks, and international and local regulations, this chapter will analyze Revolut Bank experiences to shed light on key insights.

The rapid development of electronic banks poses financial and legal challenges, particularly regarding transparency. This lack of transparency negatively impacts the information available to legal authorities governing banks locally and internationally. Consequently, there is a need to identify and approve new banks for systemic and legal significance. This involves determining indicators that national supervisory authorities can use to identify systemically important institutions, as well as coordinating between fintech, big tech companies, and new banks. The emergence and proliferation of cyber e-banks pose threats to the stability and security of the financial system. This extends beyond cyberattacks to encompass the volume of operations and their impact on the banking system as a whole.

I analysis will commence by testing the hypotheses as follows; as note in the previous table (2), which represents the risk management facing Revolut Bank, the important answer to **the main hypothesis** about the importance of legislation that prevents identity theft and fraud in online banking services, as the authorities face challenges in implementing secure and authenticated digital identity procedures, which necessitates new laws. To protect electronic bank customers and ensure transparency in fees, conditions, and dispute settlement systems, we believe that Revolut Bank has responded to operational flexibility and worked to coordinate with all jurisdictions in which it operates within the European Union. Hence, we find that a large part of

the solution lies with the electronic bank. These risks are managed through committees that follow up on the expanding developments and changes in the field of electronic banking. In fact, the actions taken by Revolut Bank confirm the principle of operational flexibility, which was emphasized by The European Union lawmakers and decision-makers have enacted Regulation (EU) 2022/2554 on December 14, 2022. The European Systemic Risk Board (ESRB) expressed apprehensions on the interdependencies of financial institutions, markets, and infrastructure, particularly in the realm of information and communications technology (ICT) systems.

This could lead to systemic vulnerabilities, as localized cyber incidents could spread throughout the entire EU financial system. The ESRB warned that about 22,000 financial entities could be affected. ICT breaches in the banking industry can have ramifications beyond individual companies and spread vulnerabilities through financial transmission channels, potentially leading to an outflow of liquidity and a decline in confidence in financial markets.[322]

With the foregoing analysis, it appears that we have addressed the essence of **the main hypothesis**, which posits that Jordan lacks independent legislation for electronic banks, hindering the prevention of identity theft and fraud in online banking services. This gap in regulation, coupled with challenges in implementing secure digital identity procedures, underscores the need for new laws to safeguard electronic bank customers and ensure transparency in fees, conditions, and dispute resolution systems. Presently, the Central Bank of Jordan's directives only regulate certain operations for digital financial companies, such as remittances, without providing specialized oversight for the electronic banking sector. This regulatory deficiency highlights an incongruity in Jordanian legislation, lacking in comprehensive regulatory frameworks.

In the same context, Revolut Bank confirms, through its work mechanisms, which are clear from the previous table, the answer to **the first sub-hypothesis**, On the inverse relationship between assessing potential systemic risks associated with electronic banks and developing risk management procedures to ensure financial stability and achieving the principle of operational flexibility amid the growth of the cyber insurance market and regulatory efforts to mitigate these risks through contracting with major cyber insurance companies to mitigate cases of operational

[322] Act (3), regulation (EU) 2022/2554 of the European parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

failure and cyber attacks. In addition to, Revolut has a well-defined timeframe for monitoring and identifying early signs of important regulatory, legislative, and political events or modifications. Revolut endeavors to comply with all applicable rules and regulations and strives to foster a robust collaborative partnership with authorities. Comprehending regulatory standards might be intricate and necessitate accurate interpretation, including taking into account their fundamental essence. Revolut is dedicated to adhering to the relevant laws, regulations, and rules, closely monitoring any changes in legislation, and implementing strong systems and controls.

The researcher acknowledges the significant impact of electronic banks and their digital services, particularly across borders, on the growth and advancement of the cyber insurance market. It seems that legislators in the European Union have emphasized the importance and growth of the cyber insurance market, which provides protection and gives confidence to customers, through Article (2) " The insurance sector has also been transformed by the use of ICT, from the emergence of insurance intermediaries offering their services online operating with InsurTech, to digital insurance underwriting.[323]" This trend has prompted a critical reassessment of the regulation surrounding this pivotal sector of risks. This is evident from data released by specialized institutions indicating a consistent expansion in the defense cybersecurity market, fostering both flexibility and operational security. Projections suggest that this market's rapid expansion will persist in the foreseeable future. However, there remains a prevailing concern among 91% of business leaders and cyber specialists regarding the likelihood of a large-scale catastrophic cybersecurity event unfolding within the next two years. This apprehension stems from the geopolitical volatility resulting from conflicts such as the Russian-Ukrainian wars and trade tensions between the United States and China. Such concerns are rooted in past events, breaches, and security crises of the preceding century, underscoring the heightened interest and urgency surrounding the cyber insurance market.[324]

[323] Act (2), regulation (EU) 2022/2554 of the European parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

[324] According to the 2022 Official Cybercrime Report, the government's proclamation of a state of emergency in response to this assault is unprecedented. It is the first time a government has taken such action against a cyberattack. The assault was executed by the "Conti" criminal syndicate, which is associated with Russia (it is thought to be under the control of a consortium of Russian hackers and has openly expressed its allegiance to the Russian government). The syndicate is notorious for specifically targeting victims with ransomware infections. The

With the information gathered from the European Commission's report on electronic financial transactions and their regulatory frameworks, I have addressed the main hypothesis: there is legislation that limits the prevention of identity theft and fraud in online banking. This is highlighted by the challenges authorities face in implementing secure digital identity procedures and the emergence of new laws aimed at protecting electronic bank customers, ensuring transparency in fees, conditions, and dispute resolution systems. Furthermore, the European Commission's report outlines the significant risks associated with electronic financial transactions and the mechanisms for controlling them. This sets the stage for addressing the As noted in previous chapters, both the European Union (EU) and the United Nations (UN) have been actively involved in developing laws and recommendations to prevent fraud and maintain financial security. The EU focuses primarily on regional standards and directives, while the UN addresses international frameworks. This reaffirms the importance of regulatory measures in safeguarding electronic banking systems and protecting customers' interests.

It is one of the most important pieces of legislation in the EU that confronts the challenges and threats to electronic banks, and limits the prevention of identity theft and fraud in online banking services; (PSD2) is an influential EU legislation that has a significant impact on online payment transactions. It requires strong customer authentication (SCA) and calls for secure online payment mechanisms. In addition, it places great emphasis on preventing fraudulent activities and managing potential risks.[325] This includes implementing regulations to ensure secure communication between payment service providers and their customers. Furthermore, the GDPR focuses primarily on protecting data privacy, but also has implications for online financial transactions. Organizations dealing with payment data must ensure that they comply with the strict data protection rules outlined in the GDPR in order to protect sensitive customer information. European law has been comprehensive and has implemented rapid and constantly evolving measures requiring financial institutions and payment service providers to establish

criminal gang demanded a payment of 20 million Dollars from the Costa Rican government in return for data retrieval. However, the government declined to make the payment and instead proclaimed a state of emergency and initiated a battle against the gang. For further information, please refer to the article titled "How the Conti ransomware group severely damaged Costa Rica and subsequently disintegrated.

[325] The European Central Bank (ECB) Working Paper Series No. 223, May 22, 2019.p.11.

robust KYC (Know Your Customer) processes and systems to identify and report potential illicit transactions in accordance with these requirements.[326]

By reviewing the previous table, table No. (1); referred to previously in Chapter II, presents a risk map that classifies payment procedures based on their potential impact in Jordan, according to the Central Bank of Jordan.[327]

This detailed analysis of the table (1) allows to evaluate the evaluation of the advantages and disadvantages of each payment service based on several factors. It is important that the choice complies with special criteria and details, based on the type of transactions and financial services that the client wants. Money protection relates to the protection of funds within the system and usually provides services that carry The previous table shows the levels of money protection and financial integrity of electronic banking and electronic payment operations and the level of these operations in terms of rise and fall. The scope of cybersecurity, information security, access to payment systems, and interoperability, where it was found that electronic banking and electronic payment operations are all subject to rise and fall in the level of risk depending on the variables available in each electronic transaction and in each electronic bank or community, the electronic environment and means of protection. In order to meet the need for cash from customers and limited assets available for repayment in the event of the insolvency of the trustee or bank.[328]

As for the second sub-hypothesis, it revolves around regulators encountering heightened difficulties in protecting the security of customer accounts and assessing potential systemic risks linked with electronic banks. This challenge is compounded by the question of electronic banks' responsibility towards customers as dominant entities in the transaction. As discussed in preceding Chapters , while technical advancements empower e-banks to offer quicker and more efficient services, they also introduce potential risks, primarily revolving around concerns related to system failures and cybersecurity threats.[329] The relationship between banks and

[326] Review of Directive (European Union) 2015/2366 on Payment Services.
[327] Central Bank of Jordan, National System Review and Oversight Department, Sixth Report, 2021.
[328] GSM Association. *Protecting Mobile Money: How Services and Systems Can Ensure Customer Protection*. 2016, p.8.
[329] Othman, Ryan. "*The Reality of Electronic Banking Services in the Arab World*." International Journal of Economic Performance 2019, no. 3 (2019). p.7-26.

customers within contractual frameworks is determined not only by contractual provisions but also by adherence to legal controls established by legislators to ensure a balance of interests between parties and protect the stability of the banking sector. The regulatory bodies charged with supervising the banking sector play a crucial role in enforcing these rules, and any violation by electronic banks of contractual or legal provisions makes them vulnerable to legal consequences and is responsible as they are a powerful dominant party to this contract.[330]

"However, This rule increases the level of standardization of several digital resilience elements by setting more stringent demands on ICT risk management and ICT-related event reporting in comparison to the current Union financial services legislation. This enhanced level of harmonization exceeds the stipulations outlined in Directive (EU) 2022/2555. Hence, this Regulation provides a precise and detailed legal structure concerning Directive (EU) 2022/2555. It is crucial to maintain a strong link between the financial industry and the European Union's comprehensive cybersecurity framework, as specified in Directive (EU) 2022/2555. This is essential to guarantee congruence with the cyber security plans developed by Member States and to allow financial supervisors to be notified about cyber events that affect other sectors covered by the aforementioned Directive.".[331]

The reputation of electronic banks can be impacted by their history of customer care and handling of client grievances. Traditional banks may have a larger customer base and face more complaints, but they also have more knowledge and resources to successfully address these issues. In contrast, online banks have a limited number of customer service staff that struggle to match consumer expectations during peak hours. Traditional banks offer a wide range of services, such as investment services and small business loans, which may make them more appealing to specific groups of consumers compared to online banks.[332]

---

[330] Fadel, Bani Muhammad. "Electronic Banks: What They Are, Their Transactions, and the Problems Raised by Dealing with Them." *Journal of Jurisprudence and Law* no. 39 (2016), pp. 44-53.
Retrieved from http://search.mandumah.com/Record/728088

[331] Act (16) , regulation (EU) 2022/2554 of the European parliament and of the council, of 14 December 2022, on digital operational resilience for the financial sector and amending regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[332] Al-Hujaila, Sahar Ayman, and Khaled Abu Al-Ghanem. "The Impact of Electronic Management on the Reputation of Jordanian Islamic Banks." *Amman Arab University Research Journal: Administrative Research Series* 7, no. 2 (2022), pp. 9-33.

However, particular banks may attract new consumers from particular groups by excelling in online savings accounts and mobile payment options. Online banks risk having their reputations damaged due to data breaches and other security issues. A growing number of clients are concerned that a significant breach may expose their personal and financial information, severely damaging the bank's reputation. The peculiar dangers that electronic banks (or e-banks) confront stem from the fact that they are so reliant on technology and online transactions. A Forbes article from 2021 states that the ease and low cost of internet banking are contributing to their rising popularity. Nearly half of all customers are considering making the move to online banking, according to a poll by PricewaterhouseCoopers. Online banks are investing heavily in the creation of digital service apps and intuitive smartphone applications.[333]

On the other hand, The bank's image may be affected by factors such as customer service, product offers, and security breaches, both in traditional and technological contexts. With the increasing number of clients transitioning to online banking, the expectation is that the reputation of e-banks would enhance. However, it is crucial for these institutions to uphold exceptional customer service and stringent security measures to sustain this confidence.

However, given the relatively young industry and the potential for cyberattacks, cyberbanks may be subject to greater surveillance[334], Another significant contrast lies in the realm of regulatory supervision, with both traditional and electronic banks being subject to government regulations. However, electronic banks may encounter a higher degree of vulnerability to cyber hazards. Regulatory supervision of electronic banks is essential for safeguarding the integrity and soundness of the financial sector. E-banks are subject to same regulations as traditional banks, but their online business model exposes them to additional risks, which may result in more extensive audits. E-banking is very vulnerable to cyber-attacks, which pose a significant and grave threat.[335]

In terms of securing consumer data and preventing illegal access to their systems, it is essential that e-banks have strong cybersecurity measures. Regulatory authorities play a crucial role in

[333] Forbes is an American media publishing company, and its most prominent publication is Forbes magazine, which is considered a good magazine in the world. Financial services to attract customers .

[334] Belhassan, Mohamed, Tarash, Hala. 2020. Factors affecting Algerian bank customers' use of electronic banks: an experimental study. Knowledge Collections, Volume 6, pp. 290-306.

[335] Zidane, Muhammad; Hamo, Muhammad. Economic insights. A. 8 (June 2015), pp. 161-181.

ensuring that e-banks meet cybersecurity standards and are prepared to deal with any cyber risks that may arise. It is essential that anti-money laundering/KYC requirements apply to e-banks as well, to prevent their exploitation for illegal purposes such as Money laundering and terrorist financing. Banks should have systems and processes in place to identify and verify customers, monitor customer transactions, and report suspicious behavior to regulatory authorities Under these requirements, that e-banks should follow consumer protection laws, capital and liquidity requirements, privacy laws, and international laws[336]. These requirements complicate the regulatory compliance environment for e-banks, yet they are vital to protecting the integrity and stability of the financial system.[337]

Consequently, the researcher asserts that regulatory monitoring is crucial in order to verify that e-banks comply with relevant laws and regulations and maintain public confidence. In order to safeguard the financial information of their clients, electronic banks must establish close collaboration with regulatory authorities to comprehend and adhere to the expanding regulatory framework. Additionally, they must allocate resources towards implementing advanced security measures and compliance systems.

Indeed, the shift towards electronic banking services within traditional banks has significantly influenced the emergence of independent electronic banks. Examples include electronic banking savings, profits facilitated through electronic wallets, and customer services for electronic payment operations offered by various companies. Through these services, transfers from accounts and deposits can be seamlessly conducted online. It's important to note that without these electronic transactions facilitated by traditional banks, the landscape would have been markedly different, potentially resulting in a more cumbersome and slower process for financial transactions.[338]

As a result, the researcher posits that the development of legislation regulating electronic banks is an unavoidable necessity given the escalating challenges in this rapidly expanding sector. The

---

[336] Hijab, Ikram, Ayad Al-Saadi, and Hussein Tayoub. "The Challenges of the Electronic Payment System and the Reality of Its Application in Algerian Banks." *Journal of International Economics and Globalization* 3, no. 2 (2020). p.130-142.

[337] Thakur, Anjan F., and Arnaud Butt. "Banking Regulation and Banking Stability." *SSRN e-Journal*, January 7, 2014, p. 7.

[338] Badawi, Bilal Abdul Muttalib. *Electronic Banking: What It Is, Its Transactions, and the Problems It Raises*. In *Electronic Banking Between Sharia and Law*. Dubai, 2003, p. 18.

proliferation of these banks is attributed to the substantial increase in electronic transactions conducted over the Internet, which forms the foundation of electronic banking operations. Electronic banks are not merely an evolved version of traditional banks; rather, they represent a novel amalgamation of advanced and systematic banking practices characterized by speed and precision. Governments must facilitate core processes to foster the growth of e-banks and online transactions while ensuring that e-banks uphold their responsibility to customers as a potent and influential entity. This underscores the urgency of developing legislation to regulate electronic banking practices.

When it comes to liability for damages, both the electronic bank and the customer often contribute to the causes of an issue, making the determination of causal relationships quite complex. Damage can stem from multiple reasons, rather than just one, and errors can lead to subsequent damages in what is known as the succession of damages. Determining the criterion for the causal relationship between the bank's fault and the customer's damage requires careful consideration.

For the customer, the individual who made the error is typically different from the one who suffered the resulting damage. However, there are instances where the wrongdoer and the affected person are the same individual. In cases where a person's mistake leads to harm to themselves personally, there is no obligation for that person to compensate another. Instead, the individual who contributed to the error bears the burden of the damage suffered without recourse to others for compensation.

Within the framework of the bank's civil liability, if the bank's mistake is caused by the customer's error, the bank's responsibility may be replaced by that of the customer who caused the harmful result through their actions. For example, if a bank grants a loan to a customer but negotiations are interrupted due to the customer's failure to provide necessary documents, the customer's mistake becomes intertwined with the bank's mistake as it was the bank's inability to complete the negotiation process that led to the interruption.

As a result, Regarding the bank's responsibility, establishing a causal relationship is a crucial condition that must be met. The customer must prove this link, recognizing the unified responsibility of the bank as a producer of services. The bank's civil responsibility is akin to that of other producers, and its professional capacity is considered fundamental. Therefore, the

bank's responsibility is professional, similar to that of a doctor or lawyer, with its specific elements integral to its existence and non-existence.

The answer to the **third sub-hypothesis** is that additional qualification requirements are needed for employees working in electronic banks related to preventing involvement amid accelerating threats such as money laundering.

The answer to this hypothesis suggests that electronic banks face significant challenges in enhancing employees' knowledge and providing them with adequate anti-money laundering (AML) training. Proper training is crucial to ensure that employees understand the risks and regulations surrounding AML practices and their role in preventing such activities. The responsible bank should issue instructions and ensure that employees stay updated on technical developments through scenario-based training sessions that enable them to practice detecting and responding to suspected money laundering activities.

Clear reporting methods, employee engagement, and safeguards to prevent financial crimes should also be established. Personalized training modules and simulations using technology-based platforms can enhance effectiveness and relevance. Strengthening interdepartmental communication and cooperation is essential to bolster AML measures. Collaboration with industry and law enforcement associations can aid in designing more comprehensive and ethically sound training programs.

By fostering a culture of compliance and providing comprehensive training, electronic banks can empower their employees to combat money laundering effectively. A comprehensive and advanced training program, combined with cutting-edge technology and robust regulatory frameworks, As is the case in the case study of Revolut Bank in Table No. **(**2**)**, or the risks of external fraud, its mitigants, and controls, its emergence bank has worked to train employees**"** The group is addressing the particular high risks by implementing compulsory training for all workers and utilizing specialized Key Risk Indicators (KRIs) to detect patterns in fraudulent incidents.[339]**"** can reduce the likelihood of financial crime in the electronic banking sector. Previous studies have highlighted that employees may not always possess the necessary capabilities to perform their roles adequately. Factors such as the efficacy of control systems

[339] Table No. **(**2**)**, Revolut Bank.

and the availability of requisite technology can influence their ability to assess risks within a company.[340]

It is important that frontline employees who deal directly with customers have the skills to assess customer risk levels, including money laundering risks. The specific responsibilities of employees whose job is to receive transactions in the electronic banking sector can vary according to the job title, type and size of the financial institution, the level of responsibility of the employee and the overall goal of ensuring the safety and smoothness of the processing of financial transactions. Furthermore, individuals working in this field must remain adaptable and stay abreast of industry developments, as banking technology and practices are continuously evolving. This includes adhering to internal rules and regulations governing electronic banking transactions, verifying customer identities, and following authentication protocols. They must also adhere to established protocols and security measures to prevent fraud and errors, troubleshoot technical issues related to transaction processing, and provide customers with clear instructions on utilizing electronic banking services.

Maintaining awareness of security protocols is crucial to safeguard against unauthorized access and fraud. To effectively assess money laundering risks, employees must understand the unconventional thinking patterns of money launderers. The ability of first responders to evaluate the likelihood of money laundering is paramount. Regulatory elements such as compliance and internal control systems, along with external variables like regulatory obligations, impact this efficacy.

As the first line of defense against money laundering, officers tasked with researching how financial institutions assess risk play a pivotal role. There is also an opportunity to address the challenges encountered by financial institutions in ensuring that frontline staff adequately assess money laundering risks.[341].

As a result, employees of digital financial institutions, especially electronic banks, require advanced and adaptable training commensurate with the pace of accelerated technology. This

[340] Simwayi, M., and G. Wang. "The Role of Money Laundering Reporting Officers in Combating Money Laundering in Zambia." *Investment Compliance Journal* (2011), p. 51.
[341] Favarel-Garrigues, G., T. Godefroy, and P. Lascoumes. "Gatekeepers in the Banking Industry: Private Actors and Anti-Money Laundering in France." *British Journal of Criminology* (2007), p. 11.

presents one of the most important challenges facing electronic banks: acquiring knowledge about warning signs in electronic transactions that may indicate the possibility of money laundering, such as suspicious account activity, strange transaction patterns, or other indicators, especially concerning cross-border remittances that may aim to finance terrorism. To identify cases of online banking fraud, technological means are necessary to detect irregularities and trends in online purchases. Advanced technological analytics, machine learning algorithms, and artificial intelligence systems must be utilized. Financial institutions can leverage these technical tools to filter vast amounts of data in search of potential indicators of money laundering. One of the most stringent anti-money laundering (AML) requirements for financial institutions is to have strong systems to detect and prevent money laundering operations. Electronic bank employees represent a real and serious challenge in money laundering cases, as the ever-changing nature of money laundering risks sometimes makes the electronic bank unwitting partners in money laundering and terrorist financing without knowledge or intention. This dilemma presents a crossroads: proceed cautiously or not deal with electronic banks to avoid fraud and data theft. The European legislator has demonstrated its commitment to digital operational resilience in the financial sector through the enactment of regulation (EU) 2022/2554. This regulation, which was issued by the European Parliament and the Council on 14 December 2022, amends several existing regulations including (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014, and (EU) 2016/1011. Unlike other countries, the Jordanian legislature has taken a cautious and gradual approach in this field. They have refrained from granting licenses to electronic banks so far, only allowing licenses for electronic payment firms and digital remittance companies. The lack of specific regulation regarding electronic banking in Jordan, specifically in relation to the Jordanian Electronic Transactions Law No. 15 of 2015

and the Jordanian Banking Law No. 28 of 2000 and its amendments, highlights the need for sufficient time to consider the experiences of developed countries such as the European Union, which achieved operational flexibility through legislation regulating digital financial operations and licensing electronic banks, as exemplified by Revolut Bank.

The answer to the **fourth sub-hypothesis;** regulators need to develop comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as operational failure or cyberattacks that could disrupt the financial system.

The answer will be through what Revolut Bank table (3) has created an operational resilience framework that is consistent with the requirements in European legislation for operational resilience[342], to confront operational failures and comprehensive crisis management strategies for electronic banks in order to deal with scenarios such as cyber-attacks that could disrupt the system. Financial. This document establishes rules, processes, and governance frameworks that allow us to effectively monitor and manage the resilience of the business services that are of utmost importance to our clients. The solution is shown by the significance and necessity of an operational resilience framework, including nine pillars of capabilities that encompass various possible causes of operational disruption and assist us in finding "resilience practices" within each pillar. Revolut has a variety of business continuity plans and disaster recovery plans in place. These plans include methods to restore company operations and technology, ensuring that services can be resumed promptly. These designs undergo frequent testing to ensure they continue to be suitable for their intended use. A Director of Operational Resilience is responsible for overseeing the framework throughout the Group and its local organizations.

In terms of the Jordanian legislator, it's I can't deny that the Central Bank of Jordan has taken significant steps in the right direction. One of the most important initiatives was the establishment of the regulatory laboratory, designed to create an experimental regulatory environment for entrepreneurs and developers to test digital financial applications in real-world settings. This initiative aims to support and encourage innovation and development in financial

[342] Act (4) The European Parliament and Council passed Regulation (EU) 2022/2554 on 14 December 2022. This regulation focuses on ensuring digital operational resilience in the financial sector. It also includes amendments to Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011. The official journal reference for this regulation is OJ L 333, published on 27 December 2022, with page number 2. In recent years, there has been a growing focus on ICT risk by international, Union, and national policy makers, regulators, and standard-setting agencies. This emphasis is aimed at improving digital resilience, establishing standards, and coordinating regulatory and supervisory efforts. The Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, the Financial Stability Board, the Financial Stability Institute, as well as the G7 and G20, work together to provide regulatory bodies and market participants in different countries with resources to strengthen the stability of their financial systems. The motivation behind that study has also been influenced by the necessity to thoroughly evaluate ICT risk within the framework of a highly linked global financial system and to strive for more uniformity in relevant best practices.
"

technology, ultimately enhancing competitiveness in the digital financial services sector, improving access to digital financial services, enhancing stability, and safeguarding the rights and data of financial consumers. This is a crucial step in encouraging investment and opening new avenues to inject financial liquidity through financial technology, particularly by enabling exchange companies to facilitate investment.

Furthermore, as highlighted in Chapter Three, the Cyber Incident Response Unit for the financial and banking sector, established within the Central Bank of Jordan, aims to strengthen the cybersecurity system for the financial and banking sector. It seeks to enhance readiness and the ability of the sector to face and respond to cyber risks. However, while these initiatives are commendable, the question remains: Are they sufficient to pave the way for the establishment of electronic banks in Jordan.

It's worth considering why the Central Bank has not implemented specific legal regulations to address the challenges facing electronic banks and outline the conditions for their licensing. Such regulations would play a pivotal role in opening the door for the establishment of new electronic banks in Jordan. By doing so, Jordan could take a significant step forward in attracting external liquidity and fostering wide-ranging investments from large companies in the electronic banking sector [343].

The answer to **Sub-hypothesis fifth**; There is a need for international coordination and cooperation between regulatory bodies for the sound international governance of electronic banks, which may lead to a mix of legislative regulations; And different jurisdictions to adapt and determine the jurisdiction and appropriate standards for disputes involving electronic banks. In fact, European Union legislators emphasized the issue of international coordination and cooperation between regulatory bodies, and it was applied effectively. This appears in the laws that encourage operational flexibility, the most important of which was in Act (14) "A Regulation helps reduce regulatory complexity, fosters supervisory convergence and increases legal certainty, and also contributes to limiting compliance costs, especially for financial entities operating across borders, and to reducing competitive distortions. Therefore, the choice of a Regulation for the establishment of a common framework for the digital operational resilience

[343] Previous reference: The official website of the Central Bank of Jordan, https://www.cbj.gov.jo/Default.aspx

of financial entities is the most appropriate way to guarantee a homogenous and coherent application of all components of ICT risk management by the Union financial sector".[344]

The survey of the structure of EU financial intelligence units (FIUs) raises questions about their operational independence and autonomy. Despite being labeled as "independent," many FIUs are part of governmental bodies in ten different countries. For instance, in Italy, the FIU operates under the Central Bank, while in Hungary, it falls under the Tax Service, and in Bulgaria, it operates within the Intelligence Service. Additionally, in fifteen countries, the responsibility for anti-money laundering and banking supervision lies with the national central bank, while in the remaining eleven, a separate financial conduct authority oversees this task. The ability of these authorities to act independently from governments and political influences is crucial. While various structures may be effective in different contexts, maintaining independence ensures impartiality and effectiveness. In general, banks are typically able to discern whether a transaction is legitimate, and it is their duty to report any suspicious transactions to the relevant authorities. However, some may not adequately adhere to these guidelines, potentially implicating them in illicit activities. To address potential violations of EU law, the European Banking Authority (EBA) serves as a backup plan. It has the authority to conduct investigations independently of national authorities, providing an additional layer of oversight and accountability. [345]

In fact, the actions taken by Revolut Bank confirm the principle of operational flexibility, which was emphasized by legislators and decision-makers in the European Union through, (regulation (EU) 2022) /2554 of the European parliament and of the council Of 14 December 2022). The European Systemic Risk Board (ESRB) raised these concerns about the interconnections between financial entities, markets and infrastructure, especially in information and communications technology (ICT) systems. This could lead to systemic vulnerabilities, as localized cyber incidents could spread throughout the entire EU financial system. The ESRB warned that about 22,000 financial entities could be affected. ICT breaches in the banking

[344] Act (14), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [OJ L 333, 27.12.2022, p. 4.
[345] See Article 17, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [OJ L 333, 27.12.2022, p 5.

industry can have ramifications beyond individual companies and spread vulnerabilities through financial transmission channels, potentially leading to an outflow of liquidity and a decline in confidence in financial markets.[346]

As a result, the need arises; the crucial necessity for international coordination and cooperation among regulators to effectively manage electronic banks on a global scale. It also highlights the importance of implementing a combination of legislative regulations across different jurisdictions to establish appropriate standards and jurisdictional frameworks for resolving disputes involving e-banks. Drawing from the European Union's approach and its oversight of e-banking transactions, there is a clear opportunity to learn from its advanced model in regulating electronic banks.

The researcher contends that international coordination and cooperation among regulatory bodies are imperative to ensure the proper management of electronic banks globally. By leveraging the European model as a benchmark for regulating electronic banks, it can serve as a catalyst for the Jordanian legislator to enhance its digital legal system. This transformation into legislation that fosters operational flexibility in the electronic banking sector is essential for promoting innovation and growth in this vital industry.

The answer **to the sixth sub-hypothesis**, which posited that electronic banks would encounter challenges in adhering to various financial regulations such as anti-money laundering (AML) & (KYC) requirements, necessitating the development of comprehensive strategies to manage transaction scenarios, is as follows:

As discussed in earlier chapters of this research, electronic banks must address financial rules pertaining to anti-money laundering (AML) & (KYC) requirements, while also developing robust strategies to manage transaction scenarios. Electronic banks must be well equipped to address any potential cyber dangers that may occur. AML/KYC rules are crucial for online banks to thwart their misuse for illegal activities such as money laundering and terrorism funding. In order to adhere to these specifications, he carried out the following actions, which were subsequently adopted as a European model within an electronic banking system. "Risk

[346] Act (3), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [OJ L 333, 27.12.2022, p. 2.

Revolut relies on third-party entities and external service providers for various functions, such as payment processing, adhering to regulatory requirements, conducting foreign and cryptocurrency exchanges, providing trading services, and managing KYC/AML procedures, as well as other business-related services. Electronic banks should establish robust systems and procedures to accurately identify and authenticate customers, monitor their transactions, and promptly report any potentially illicit activities to the appropriate regulatory bodies ". Moreover, electronic banks must adhere to consumer protection laws, as well as meet capital, liquidity, privacy, and international legal requirements. While these regulatory obligations may complicate the compliance landscape for electronic banks, they are indispensable for safeguarding the integrity and stability of the financial system. [347]

In fact ,the purpose of KYC is to identify the individual/company, while AML is used to protect against money laundering. We find that the European legislator has focused on legislation that leads to creating a safe environment in the electronic banking sector, and the Sixth Anti-Money Laundering Directive (6AMLD)[348] protects the landscape of AML and KYC in Europe, the Directive entered into force on 3 June 2021, and 5AMLD has been updated, adding greater clarity and helping businesses fight money laundering. The Guidelines set out a list of predicate offenses for money laundering, including fraud and counterfeiting. It also adds two new crimes to the list: cybercrime and environmental crime, indicating that crime is evolving and so are the criminals involved in it. The other directives/regulations that govern money laundering in the EU include; Payments Services Directive (PSD2), General Data Protection Regulation (GDPR), Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).

Therefore, it is essential to have regulatory monitoring in place to guarantee that electronic banks adhere to relevant laws and regulations and maintain the confidence of the public. In order to safeguard the financial information of their clients, electronic banks must establish close collaboration with regulatory authorities to comprehend and adhere to the expanding regulatory framework. Additionally, they must allocate resources towards implementing advanced security measures and compliance systems.

---

[347] Anjan F. Thakur, Arnaud Butt, Banking Regulation and Banking Stability, article in SSRN e-Journal, 2011, p. 7, Previous reference.

[348] (6th AML) Directive aims to harmonize the definition of predicate offences against money laundering by all Member States. The 22 predicate offences for money laundering now includes cybercrime and environmental crime.

Without the initial adoption and integration of electronic banking services by traditional banks, the development of independent electronic banks would have faced considerable challenges. The presence of electronic transactions facilitated by traditional banks has streamlined financial processes and paved the way for the evolution of electronic banking. This integration has played a crucial role in accelerating the transition towards electronic banking services, making financial transactions more accessible, efficient, and convenient for customers. [349]

The researcher emphasizes the necessity of developing legislation to regulate electronic banks, considering the sector's rapid growth and the challenges it presents. The proliferation of electronic transactions on the internet forms the foundation of electronic banks, driving their expansion. However, electronic banks are not merely advanced versions of traditional banks; they represent a fusion of advanced technology and systematic banking practices that prioritize speed and precision. To facilitate the growth of electronic banks and online transactions, governments must play a proactive role by enabling essential processes. This includes the development of comprehensive strategies to manage the diverse transaction scenarios encountered in the electronic banking landscape. By establishing clear regulatory frameworks and implementing supportive policies, governments can foster an environment conducive to the expansion and effective functioning of electronic banks.

As a general result, and through what was discussed in the dissertation, it emphasized the profound impact of the European Union rules on the Jordanian legal frameworks, with a focus on how these laws affect the formulation and implementation of the Jordanian Electronic Transactions Law. It critically assesses the viability of EU law as a comparable benchmark for Jordan, considering the country's non-EU status and distinct socioeconomic circumstances. Furthermore, the dissertation investigates the extent to which Jordanian regulations fit with global banking service needs, highlighting both the progress made and the problems encountered in reaching regulatory compliance with international standards.

The analysis of the impact of EU regulation on Jordanian regulation is rooted in the unique nature of this relationship and its broader implications for Jordan’s regulatory framework. EU regulations often serve as a benchmark or reference point for non-EU countries, particularly in

[349] Badawi, Bilal Abdul Muttalib. *Electronic Banking: What It Is, Its Transactions, and the Problems It Raises*. In *Electronic Banking Between Sharia and Law*. Dubai, 2003. p. 18. (Previous reference).

regions seeking to align with international standards such as Jordan. In fact, this analysis aims to highlight the ways in which EU regulatory frameworks influence Jordanian law, whether through direct adoption, indirect harmonization, or comparative divergence; such a focused discussion is particularly relevant given Jordan's engagement with international regulatory frameworks and its efforts to modernize its legal system in line with global standards. This analysis allows for a comprehensive exploration of these dynamics without conflating them with broader domestic regulatory developments; this is what was confirmed by the two most important hypotheses (the seventh and eighth) on which the research was based, which state the following; **Seventh Sub-Hypothesis :**Is the Jordanian Electronic Transactions Law compatible with European Union and international standards, and **eighth Sub-Hypothesis;** the extent to which EU regulations affect Jordanian regulatory frameworks, particularly in the context of challenges related to digital banking services, in terms of EU legislation being the most appropriate standard for Jordan, given its membership outside of the EU, and how the Jordanian banking system also meets the requirements of the global banking system.

V.2 The Findings

As a final result, the answer to **the main research question** is to what extent does the Jordanian Electronic Transactions Law conform to the rapid legislative developments in this sector in light of the transformation of international standards and the European Union to confront the emerging challenges of electronic banks, i find the answer, and through what was previously mentioned in the research, it can be summarized briefly; The researcher confirmed that one of the most important results reached by this research is the lack of compatibility and coherence in Jordanian legislation, and this is particularly evident in the Jordanian Electronic Transactions Law No. 15 of 2015 and the Jordanian Banking Law, and in fact, these results answer one of the most important opportunities, which is the focus of **the seventh sub-hypothesis** on the extent to which the Jordanian Electronic Transactions Law conforms to the European Union and international standards, which is closely related to the main research question, as these laws noticeably omit any mention of legal regulations related to digital or electronic banks, and instead refer primarily to electronic companies or electronic providers, which confirms the lack of synchronization regarding the concept of electronic banks within the Jordanian regulatory

frameworks. At the same time, the Central Bank of Jordan recently indicated its approval of electronic services, even under the name of electronic companies, electronic payments, or digital financial transfers. This cautious approach adopted by legislators and decision makers at the Central Bank indicates an unwillingness to fully adopt electronic banking services, and this represents the answer to **the first sub-question** to what extent the Jordanian Electronic Transactions Law is compatible with the rapid legislative developments of electronic banks in light of international regulatory developments and the European Union.

However, this cautious stance could potentially lead to legal disputes in the future, as the absence of explicit references to electronic banks in the legal framework may pose challenges for adjudication. Should such disputes arise, judges may be compelled to interpret existing laws, such as the Jordanian Electronic Transactions Law No. 15 of 2015, which lacks specific provisions related to electronic banks. This legislative deficit necessitates urgent attention from lawmakers to align Jordanian legislation with international standards, particularly drawing from advanced models such as the European framework for licensing and establishing electronic banks. Such efforts are crucial to motivate decision-makers in Jordan to facilitate the entry of electronic banking into the market; after reviewing the nature of electronic banks and their legislative organization in Jordan, the research reached the following results:

Jordan's Electronic Transactions Law is generally devoid of any legal provisions specifying the conditions for cases in which the documents submitted are responsible, and the legislator has only included provisions establishing a criminal penalty for issuing an inaccurate, suspended, or canceled certificate of authenticity.

The EU Directive on unfair terms provisions of 5 April 1993 can be applied to the relationship between customers and suppliers.

The Electronic Transactions Law does not address the civil liability of authentication service providers, because the Jordanian legislature did not regulate the subject with special provisions. Rather, regulations were limited to electronic systems and imposed financial penalties and fines for providing false data.

The Jordanian legislator has not established a specific legal regime for the liability of the electronic authentication provider and the third party to clarify all ambiguities.

The Jordanian Electronic Transactions Law does not clearly, precisely and in detail explain how to grant an electronic certificate. Here we find one of the answers addressed by the **second sub-question** about what the weaknesses of the Jordanian Electronic Transactions Law in light of the international model and the European Union directives .

The digital economy has unleashed significant opportunities for growth and innovation, spanning from online shopping and mobile banking services to a plethora of payment applications. Electronic payments have revolutionized daily transactions, offering convenience and speed. Recognizing the transformative potential of financial digitization, legislators, particularly central banks, prioritize regulating legislation to facilitate investment in the electronic banking sector.

The online payment risk landscape is still complex. The risks associated with electronic payments can be categorized into several concerns, whether they are related to security, privacy, technological challenges, or regulatory compliance. This answer, which expresses the most important one of the hypotheses, which is the **sixth sub-hypothesis**, is that electronic banks will face difficulties in complying with many financial rules, such as anti-money laundering and know-your-customer requirements, and the need to develop comprehensive strategies to manage their transaction scenarios.

Jordan has made significant progress in regulating the payments system and ensuring its security by licensing companies through the Central Bank to operate in payments and remittances. However, it has yet to establish regulations specifically tailored for electronic banks.

Money laundering threatens both financial institutions and national security, as it allows criminals to disguise illegal funds as legitimate. Electronic banks are particularly vulnerable to the risks associated with money laundering.

Electronic banking operations play a vital role in economic development by streamlining processes, saving time and money, and enhancing efficiency. Despite their benefits, they are susceptible to tampering and cyber-attacks.

Ensuring criminal protection for electronic banking services is crucial for building trust between companies and customers.

In Jordan, criminal protection for electronic banking operations is outlined in Articles 6 and 7 of the Cybercrime Law; article (6 +7) of the Jordanian Electronic Crimes Law stipulates the following, article (6) Anyone who intentionally obtains, without permission, through the information network or any information system, data or information related to credit cards or data or information used in executing electronic financial or banking transactions shall be punished with imprisonment for a period of not less than one year and not more than three years and a fine of not less than (500) five hundred dinars and not more than (2000) two thousand dinars. Article (7) Anyone who commits any of the acts stipulated in Articles (3), (4), (5) and (6) of this law if they occur on an information system, electronic website or information network related to the transfer of funds, or the provision of payment, clearing or settlement services or any of the banking services provided by banks and financial companies shall be punished with temporary hard labor for a period of not less than five years and a fine of not less than (5000) five thousand dinars and not more than (15000) fifteen thousand dinars, while Jordanian legislation provides some level of criminal protection for electronic banking services, it falls short of comprehensive protection. The law should encompass all electronic cards, including bank cards, and criminalize activities such as card fraud and the use of counterfeit or stolen cards, mirroring the approach taken by the European legislator. As a result, decision-makers and legislators must amend these articles to include real criminal protection for all potential electronic operations and attacks that threaten the financial system, and should not be limited to what is mentioned only in Article (6 + 7), which may not cover all cases of expected threat, such as impersonation, data theft, and all hacking operations that may be carried out. Legislators must have automatic procedures and precautionary measures in this regard after an analytical study of all cases of expected threat to the electronic financial system.

Jordanian legislation lacks independent legal provisions for resolving disputes related to electronic transactions. Establishing uniform legal procedures and regulations for chargebacks and dispute resolution would mitigate conflicts between consumers and merchants, similar to measures implemented by the European Commission to address disputes within the European Union, as exemplified in the case research of Revolut Bank.

V.3 The Recommendations

Based on the search for the research, the researcher recommends the following:
In response to the changing landscape of digital finance and electronic economic technologies, the Jordanian legislature should re-evaluate and improve the existing legal structures to ensure their relevance and efficiency. This research proposes several suggestions to improve the framework for digital business in Jordan.

First, it is important to update the Jordanian Electronic Transactions Law No. 15 of 2015 and the Jordanian Banking Law to reflect the improvements in electronic business technologies. This includes the establishment of a body composed of representatives from various regulatory authorities and banks to regularly review and amend these regulations, and periodically directly proportional to the developments of financial technology. Following the EU strategy of focusing on the constant development of regulations to control electronic economic procedures, Jordan needs to take a similarly aggressive stance. In doing so, the country can minimize potential threats to economic and financial security that arise from outdated policies in the rapidly evolving e-business landscape, opening the door to licensing independent electronic banks to increase flow, liquidity and investment in Jordan.

In addition, there is an immediate need for specific regulations outlining the obligations of digital paperwork associated with verification companies. Without clear legal structures regulating their procedures, there is unpredictability regarding the obligations of digital purchases. Therefore, Jordanian lawmakers need to develop specific legal regulations for the obligations of these providers, utilizing the ideal methods from around the world, especially the EU.

Furthermore, amendments to the existing cybercrime regulations are essential to cover all facets of digital financial procedures. The overlap between different pieces of legislation can lead to confusion and also inefficient enforcement. By amending relevant sections, such as Article 6, to ensure comprehensive insurance coverage for digital financial transactions, the legal structure can successfully combat cyber threats as well as unauthorized access to economic systems.

It is important for regulators to consider the balanced model of e-banking, which aims to address various concerns such as protecting customer rights, the interests of e-bankers and investors, and economic variables.

I suggest too, increase collaboration with fintech companies to streamline transaction processes and explore potential synergies in underserved markets.

There is no doubt about it, that regulators, especially central banks, should clarify how to achieve a level playing field between traditional and electronic banks. This involves addressing issues such as licensing, capital requirements, competitiveness, and the benefits of moving from the traditional environment to digital finance.

In addition to the above resolving civil law issues related to verification companies is another important aspect of interest. Existing policies mostly concentrate on digital systems and impose fines for providing false information, but do not address the civil issues. Therefore, the Jordanian legislator needs to create specific regulations to clarify the legal obligations of verification companies to promote reliability and self-confidence in digital transactions.

Moreover, the integration of legal guidelines to ensure compliance with anti-money laundering (AML) and customer identification (KYC) requirements is crucial. Given the cross-border nature of digital finance, Jordan needs to align its regulatory structure with global criteria to prevent illicit money transactions and enhance customer security.

I suggest that the Jordanian legislator focus in a consistent manner with the rapid technological development on a deep analytical discussion of the civil and criminal liability of service providers in light of the issue of the responsibility of electronic banks towards customers as a strong and dominant party.

Indeed, developing comprehensive crisis management strategies for electronic banks needs to be proactive in order to deal with scenarios such as operational failure or cyber-attacks that may disrupt the financial system. Accordingly, I recommend that decision-makers develop risk management procedures to ensure financial stability in light of the growth of the cyber insurance market in Jordan, and to regulate it with an independent law to reduce risks.

In general, security in electronic payment systems is of paramount importance, and it is necessary to combine legal regulations, compliance enforcement and ongoing security measures to mitigate the risks associated with cyber threats in the financial sector.

In the same context, as the cybersecurity threat landscape is always changing, efforts must be made to continuously improve security and legislative updates. The Jordanian legislator should also encourage regulations to encourage payment service providers to regularly update and improve their security procedures in order to remain vulnerable to new threats. Indeed, the Central Bank of Jordan and the Jordanian legislator should highlight this matter, by making sufficient efforts to fully educate consumers about the risks and importance of cybersecurity and raise awareness in the Jordanian society.

In fact, electronic payment methods have created a new set of risks that require careful research and regulation, and the Central Bank of Jordan is continuously supporting the transition from the traditional paper payment system to a more advanced electronic payment system. It is actively looking for opportunities to promote investments in the development of electronic payments and is developing a regulatory framework for their management. This development is crucial for ensuring that electronic banking operations are conducted within a robust legal framework, thereby promoting the growth and stability of the digital financial sector in the country.

Last but not least, staff training and development is crucial to improve the efficiency of digital financial procedures. Employees in e-banks must be equipped with the necessary expertise and skills to successfully identify and minimize money laundering threats. By focusing on training their employees, digital financial institutions can increase their functional honesty and protect themselves from white-collar crime

Finaly, the proposed legislative reforms aim to modernize and strengthen the digital finance environment in Jordan. By updating existing regulations, establishing clear legal obligations, and improving regulatory compliance, Jordan can cultivate electronic economic innovation while protecting itself from potential threats and dangers. Jordanian lawmakers should act with vigor and work with stakeholders to implement these reforms while ensuring the sustainable development of the digital finance industry.

Bibliography

1. English References

- Anjan F. Thakur and Arno Butt, "*Banking Regulation and Banking Stability* " *SSRN e-Journal* (January 7, 2014).

- Cedric J. Magnin, "*The Telephone Banking Contract in Swiss International and Comparative Law*," *ILSA*, 2001.

- Cora, N. A. Economic Computer Crimes: *A Theoretical and Applied Study*. Arab Renaissance House, 2003/2004.

- De Kock, R. Central Banking. *Translated by Abdul Wahed Al Makhzoumi. Vanguard Publishing House, Beirut, 1987, 30.*

Dubois, K. Gleeson. *"Cryptocurrency Money Laundering: Open Doors and Regulatory Dilemmas*." Financial Crime Journal (2020): 13.

- Favarel-Garrigues, G., T. Godefroy, and P. Lascoumes. *"Gatekeepers in the Banking Industry: Private Actors and Anti-Money Laundering in France."* British Journal of Criminology (2007): 11.

- Gerbrands, F., P. Unger, M. Getzner, and J. Verwerda. *"The Impact of Anti-Money Laundering Policies: An Empirical Network Analysis*." EPJ Data Science 20 (2022).

- Ghulam, M., A. Lowland, R. B. Housby, and J. Ononsen. *"Detecting Money Laundering Transactions Using Money Laundering Machine Learning."* (2020).18.

Gilmore, Evening. "Rethinking the AML Framework: A Legal Critique and a New Approach to AML." Financial Crime Journal (2022).25.

- Harding, N., and K. T. Troutman. *"Enhancing Auditor Competency Ratings: Another Look."* Auditing: A Journal of Practice and Theory 28, no. 1 (2009). 53-78.

- Heti, M. H. M. Information Crime: Examples of Its Applications. 2nd ed. Legal Books House, 2014.Kalink, Z.; Marinkovic, F. Molinello, S. Liébana-Cabanillas, *F. (2019) A multi-analytic approach to predicting peer-to-peer mobile payment acceptance. J Retail. consumption. gifts, s. 13.*

- Ianchovichina, Elena. *"A Return to Political Stability Will Solve the Economic Problems in the Middle East and North Africa."* Arab Voices Magazine, November 1, 2013.

- J.C. Christiano, J. Ehrentraud, and M. Fabian, *"Big Tech in Finance: Regulatory Approaches and Policy Options,"* FSI Briefs *No. 12 (Basel, Switzerland: Bank for International Settlements, 2021), available at: https://www.bis.org/fsi/fsibriefs12.pdf (accessed January 13, 2023).*

- Kavitha Vani, S. D. *"Electronic banking Modules: Perception and Acceptance of Customers in Rural India." IUP Journal of Bank Management* 21, no. 4 (November 2022): 7-26.

- Kavitha Vani, S. D. *"Electronic banking Modules: Perception and Acceptance of Customers in Rural India*." Journal of Bank Management 21, no. 4 (November 2022): 10.

- Koshy, S. "*Find Rotten Eggs at the Right Price*." Compliance Clinic (2010): 44-46.

- Kute, D. V., B. Pradhan, N. Shukla, and A. Alamri. "*Deep Learning and Explainable AI Techniques Applied to Money Laundering Detection: A Critical Review*." IEEE Access (2021): 14.

- L. Brainard, "*Cryptocurrencies, Stablecoins and the Evolving Payments Landscape," Notes on the Future of Money in the Digital Age*, Washington, DC, October 16, 2019, available at: https://cutt.us/ZJZEv (accessed October 22, 2023).

- Laguna de Paz, J. C. "*Some Implications of the New Global Digital Economy for Financial Regulation and Supervision*." Journal of Banking Regulation (2023): 11.

- Laksana, Rio Danny, Intan Shaveri, and Humira Nazini. *"The Impact of Operational Risks on Electronic banking Services in Banks."* Journal of Business Administration 14, no. 2 (2023): 459.

- Lim, C., P. T. Futseng, A. Al-Masry, O. Musa, M. L. M. Kia, T. F. Ang, and R. *Ismail. "Blockchain Technology Disrupts Identity Management and Authentication Service: A Survey*." International Journal of Advanced Science, Engineering and Information Technology (Malaysia), 17 (2018).
- Lopez, M. R. "*Law Enforcement Agencies Recognize the Crime of Money Laundering Based on Pancasila*." In J. Hawk (Ed.), UNISSULA, 38, no. 1 (2022): 24.
- Mill, B., J. Dry, and J. Schock. "*Federated Identity Management for Smart Contracts Without Third-Party Authentication Services*." Bonn, 2019, 7.
- Mill, P., J. Dry, and J. Schock. *"Unified Smart Contract Identity Management Without Third-Party Authentication Services*." Bonn, 2019, 15.
- Mufti, Mohamed Salah. "*Electronic Banking Services." Finance and Economics* (2013): 72, 36-38.
- Othman, Ryan. "*The Reality of Electronic Banking Services in the Arab World."* International Journal of Economic Performance (2019): 3, 7-26.
- Peter, H., Kamil, M., and J. S. "*Electronic Banking Security: A Comparative Study."* In 2nd Annual IEEE International Conference on Security Technology, Prague, Czech Republic, 2008: 326-330.
- Rusanov, J., and Podovushkin, Y. "*Money Laundering in the Modern Crime System*." Money Laundering Observatory 13 (2021).
- Saharouni, A., and Waridi, A. " ICLSSEE, May 6, 14 (2023). *Virtual Currency (Bitcoin) as a Tool for Money Laundering."*
- Schmid, J. "*How Adequate Are Efforts to Combat Money Laundering? The Jamaican Experience."* Report No. IDB-PB-242, Inter-American Development Bank Country Policy Briefs (2015): 9.
- Simwayi, M., and G. Wang. "*The Role of Money Laundering Reporting Officers in Combating Money Laundering in Zambia."* Investment Compliance Journal (2011): 51.
- Tiwari, M., A. Gibb, and K. Kumar. "*Review of the Literature on Money Laundering: State of the Art Research into Key Areas."* Pacific Accounting Review 11 (2020).

- Van Gestel, Rob, Hans W. Micklitz, and Edward L. Rubin, eds. *Legal Scholarship Reconsidered: A Transatlantic Dialogue*. New York, NY: Cambridge University Press, 2017.
- Wronka, C. "*Money Laundering Online: Changing Money Laundering in the Digital Age* " Money Laundering Watch Journal 8 (2022).
- Zhang, L. "*Understanding the Impact of Financial Incentives on NFC Mobile Payment Adoption: An Empirical Analysis*." International Journal of Bank Marketing 37 (2019): 1298.
- Zhang, R. *"Factors Influencing Consumers' Mobile Payment Behavior: A Meta-Analysis."* Electronic Commerce 18 (2019).

2. Arabic References

- Abdel Haq, Alwa. *"Civil Liability of the Bank for Banking Errors Towards the Customer*." Faculty of Law and Political Sciences, Larbi Ben M'hidi University, Oum El Bouaghi, Algeria, 2021, p. 323.
- Abdullah Musa Alqam, "*Money and Economics*," vol. 63 (June 2010): 47-48.
- Abu Al-Lail Al-Awwal. "*Documentation of Electronic Transactions and Burning"* Their Nature and Legal Impact. 2018.
- Abu Al-Lail I., Documentation of Electronic Transactions: Burning, Nature, and Legal Effect. 2018; Brun M., "*Nature and Effects of Juridiques de la Certification in Electronic Commerce on the Internet* " March 2000. For more information, see lex-electronica.org.
- Abu Jaris, George, and Khashan Rashwan. *Introduction to Internet Banking*. Union of Arab Banks, Beirut, 2004, p. 15.
- Ahmed, H. A. A. "*Traditional and Modern Information Crimes and Their Applications in the Bahraini System*." 2013.
- Al-Aqabi, B. A., Al-Jubouri, A. A., and Jabr, N. K. "*Electronic Money and Its Role in Fulfilling Contractual Obligations.*" Ahl al-Bayt Magazine 10, no. 6 (2008): 125.

- Al-Atrash, Heba, and Belhassan, Muhammad. 2021. *Factors affecting the adoption of electronic banking services:* A quantitative study of a sample of Algerian bank customers. Journal of the Institute of Economic Sciences, M.J. 24, p. 1, pp. 167-185.
- Al-Daghim, A.A. and M. Al-Amin, "*Al-Jarro Iman: Credit Analysis and Its Role in Simplifying Banking Operations Applied in the Industrial Bank of Syria*," Tishreen University Journal for Scientific Studies and Research 28, no. 5 (2006), issue 35.
- Al-Gamal, S. "*Entrepreneurship through Modern Communication Technologies*". Dar Al-Nahda Al-Arabiya, Cairo, 2006, p. 321.
- Al-Hamoud, F. "*Credit Card Legal System"* Dar Al-Thaqafa for Publishing and Distribution, Amman, 1999, p. 15.
- Al-Hujaila, Sahar Ayman, and Khaled Abu Al-Ghanem. "The Impact of Electronic Management on the Reputation of Jordanian Islamic Banks." Amman Arab University Research Journal: Administrative Research Series 7, no. 2, pt. 2 (2022): 9-33.
- Al-Hussein, Hussein Shehadeh. "Electronic Banking Operations." In Banking Conference, Faculty of Law, University of Beirut, 2002, p. 201.
- Ali, Jamal al-Din Awad. Banking Operations from a Legal Perspective. Arab Renaissance House, 1981, p. 2.Al-Janabihi, Mounir et al. (2005), Electronic Banks, First Edition, Dar Al-Fikr Al-Jama'a, Alexandria, p. 10.
- Al-Jawarna, S.A. "*Online Banking Security Measures and Data Protection*." IGI International, 2017. https://doi.org/10.4018/978-1-5225-0864-9.
- Al-Animat, Mohammad Elayan. *"Legal Perspectives and Discrimination in Electronic and Traditional Banks*." Lex & Science International Magazine (2023): 154.
- Al-Sabahin, S. "*The Electronic Signature and Its Authenticity in Evidence*." Unpublished medical thesis, Amman Arab University for Postgraduate Studies, Jordan, 2005, p. 156.
- Al-Sharqawi, Mahmoud Ahmed Ibrahim. "*The Concept of Electronic Banking and Its Most Important Applications.*" In Conference on Electronic Banking between Sharia and Law, United Arab Emirates University, 2003, pp. 17-18.
- Al-Sharqawi, Mahmoud Ahmed Ibrahim. *Electronic Payment Systems*. 1st ed. Lebanon: Al-Halabi Legal Publications, 2008, p. 24.

- Al-Tamimi, A. *Legal Regulation of Online Banking*. Alexandria: New University House, 2012, p. 429.
- Al-Wazani, K. "*The Banking System and Monetary Policy in Jordan During the Period (1989-1990)."* Strategic Studies, University of Jordan, 1996, p. 33.
- Amer, T. Hani, Vladislav Yevseyev, Ayman Amer, Natalia Dymska, Ashish Kar, Lohash Vyacheslav Lyachenko. "*Electronic User Authentication Key for HMI/SCADA Access Over Unsecured Internet Networks.*" Faculty of Computer Science and Information Technology, Ajloun National University, Ajloun, Jordan, 2022.
- Anwar, M. "*The Urgent Need to Reform Money Laundering Regulations in the Digital Age*." East Asian Journal of Interdisciplinary Research (EAJMR) 2, no. 7 (2023): 11.
- Arab, Younis. "*Electronic Banks Between Advantages and Disadvantages*." Kenanah Information Technology Company, Jordan. Accessed May 27, 2022. www.kenanah.com.
- Aziz, Al-Ukaili. *The Expiration of the Fixed Obligation in the Check*: A Study in Comparative Legislation and the Unified Geneva Conventions. Amman: International Scientific House and Dar Al-Thaqafa for Publishing and Distribution, 2001, p. 357.
- Badawi, Bilal Abdul Muttalib. *"Electronic Banking: Its Nature, Transactions, and the Problems It Raises".* Electronic Banking between Sharia and Law. Dubai, 2003, p. 11, 18.
- Badawi, Bilal Abdul Muttalib. *"Electronic Banking: Its Nature, Transactions, and the Problems It Raises. Electronic Banking between Sharia and Law".* Dubai, 2003, p. 11, 18. Anjan F. Thakur, and Arno Bout. "Banking Regulation and Banking Stability." Article in SSRN e-Journal, January 7.
- Barba, Robert. *"The Battle for Talent Is Heating Up as Electronic banking Becomes Paramount." US Banker*, August 17, 2016, Volume 181, Issue 158, p. 1.
- Barham, Nazzal Salim. "*Provisions of Electronic Commerce Contracts".* 1st ed. Amman: House of Culture, 2009, p. 169.
- Belhassan, Mohamed, and Hala Tarsh. *"Factors Affecting Algerian Bank Customers' Use of Electronic Banks: An Experimental Study.*" Cognitive Collections, Volume VI, 2020, pp. 1, 290-306.

- Fadel, Bani Muhammad. "*Electronic Banks: What They Are, Their Transactions, and the Problems Posed by Dealing with Them*." Journal of Jurisprudence and Law No. 39, 2016, pp. 44-53. Retrieved from http://search.mandumah.com/Record/728088 .
- Favarel-Garrigues, J., Godefroy, T., and Lascom, P. "*Bank Vigilantes: Private Actors and Anti-Money Laundering in France*." British Journal of Criminology, 2007, p. 11.
- Ghannam, S. M. *The Bank's Responsibility for Computer Errors in Transferring Funds Electronically*. Cairo: University Publishing House, 2010, p. 13.
- Hafida, Qara. "*Electronic Banking and the Bank's Civil Liability Therein."* Faculty of Law and Political Science, University of Batna, Algeria, 2019-2021.
- Hamad, Tariq Abdel-Al. "*Corporate Governance: Concepts, Principles, Experiences - Applications of Governance in Banks".* University House, Cairo, 2007, p. 244, 23.
- Hamidi, N. A., Mehdi Rahimi, J. K., Navarya, A., and Robertson, B. "*Personal Security Methods in Electronic Banking Using Flask Architecture on the Cloud*." 2013.
- Hassan, L. "*Electronic Documentation and the Responsibility of Competent Authorities".* Al-Raya Publishing and Distribution House, Amman, 2009, p. 101.
- Hegazy, AFP. "*Online Consumer Protection. Alexandria* "Dar Al-Fikr Al-Jami', 2006, p. 144, 52Hegazy, W&T, Kamel, Electronic Signatures, Certification Service Providers, 2015. yorffy, J.C., Tappenden, A.F. and Miller, J. (2011) "Token-based graphical password authentication." International Journal of Information Security, pp. 1-16.
- Hijab, Ikram, Ayad Saadi, and Hussein Tayoub. "*The Challenges of the Electronic Payment System and the Reality of Its Application in Algerian Banks*." Journal of International Economics and Globalization 3, no. 2 (2020): 130-142.
- Ibrahim, A. "*Concluding the Contract through Electronic Settlement and Proving This".* Alexandria: Dar Al-Fikr Al-Jami', 2015, p. 144, 262.
- Ibrahim, K. M. "*Concluding an Electronic Contract - A Comparative Study".* Alexandria: Dar Al-Fikr University, 2006, p. 329.
- Jaber, Ali. "*Factors Influencing Adoption of Electronic banking in India: Evidence from the World Bank's Global Financial Inclusion Index Survey*." Developing Regions Journal 57, no. 2 (Spring 2023): 341.

- Kafi, Mustafa Youssef. *"Electronic Money and Banking".* 1st ed. Damascus: Raslan Publishing and Distribution House, 2012, p. 111.
- Kamel, T. "*Electronic Documentation Service Providers (Legal System, Duties and Responsibilities*)." University of Sharjah Journal of Islamic and Legal Sciences 5 (2008): 237.
- Khams, Aser A. "*The Impact of Digital Transformation on Recruitment Strategy in the Banking Sector: A Case Study for Egypt*." Journal of International Comparative Management 23, no. 3 (July 2022): 457.
- Al-Animat, Mohammad. "*Technical Protection for Electronic Banking Operations in Jordan.*" Current Law 92, no. 1 (2023): 98.
- Muhammad, Z. M., and K. Ahmed. "*Investigating Money Laundering Cases and Prosecuting Criminals in Malaysia.*" Money Laundering Monitoring 15, no. 4 (2012): 421-429.
- Mustafa, Ahmed. "Monetary Policy and Economic Growth." Jordanian Banking Journal 19, no. 5 (2000): 9.
- Olionek, S." *Law and Technology in a Global Digital Society"* . Springer, 2022. "Phishing in Online Banking – An Overview of the Development and European and German Legal Positions," May 2022.
- Omar, Muhammad. "*Dawaba Contract for Bank Transfer"* - Legal Study. Master's Thesis, 1st ed. Amman: Dar Al-Thaqafa for Publishing and Distribution, 2006, p. 193.
- Othman, Ryan. "*The Reality of Electronic Banking Services in the Arab World*." International Journal of Economic Performance vol. 2019 (2019): 7-26.
- Qasim, A. "*Some Legal Aspects of Electronic Signature*." Journal of Law and Economics no. 72 (2002): 32.
- Radwan, F. N. "*Loyalty Cards*". New Galaa Library, 1990, p. 24, 17.
- Rashid, A. "*An Analytical Study of the Phenomenon of Money Laundering".* Ministry of Finance and Department of Economy in Iraq, 2016.
- Reda, Mr. *The Banking System and Banking Operations*. 2000, p. 121.
- Sahar Ayman Al-Hujaila and Khaled Abu Al-Ghanem, *"The Impact of Electronic Government on the Reputation of Jordanian Islamic Banks*," Amman Arab University Research Journal: Administrative Research Series 7, no. 2 (2022): 9-33.

- Saladin, Hamad Saladin. *Northern Oasis*. vol. 3, no. 6 (December 2012): 36-39.
- Saleh, Ali Salman, and Rami Zaytoun. "*Islamic Banks in Jordan: Performance and Efficiency Analysis.*" Journal of Islamic Economics 11, no. 1 (2007): 49.
- Salem, M. "*Criminal Protection of the Loyalty Card".* Arab Renaissance House, 1st ed., 1995, p. 1.
- Sarhan, A., and Khater, N. "*Sources of Personal Rights".* Dar Al-Thaqafa for Publishing and Distribution, 2021, p. 302.
- Serafi, M. "*Managing Banking Operations - Regular - Exceptional – Electronic".* 2nd ed. Egypt: Dar Al-Fajr for Publishing and Distribution, 2016, p. 12.
- Simway, M., and Wang, J. "*The Role of Reporting Officers in Combating Money Laundering in Zambia.*" Investment Compliance Journal (2011): 51.
- Supriyanto, E. E., Tunda, A., and Upe, A., eds. "*Opportunities for Implementing E-Rupee Policy Innovation in Financial Transactions in the COVID-19 Pandemic*." In Global Policy in Dealing with the COVID-19 Pandemic, 1st ed., 17. Kendari: Roma Bonni, 2021.
- Thabet, F. H. "*The Impact of the Current Global Financial Crisis on the Performance of Islamic Banks and Development*." Op. cit., 2009, p. 2.
- Thakur, Anjan F., and Arno Bout. "*Banking Regulation and Banking Stability*." Article in SSRN e-Journal, January 7, 2014.
- Touqan, Umayya. "*Monetary Policy Aims to Maintain Monetary Stability*." Jordanian Banking Journal 20, no. 8 (October 2001): 26-27.
- Yacoub, A. "*Civil Liability of a Digital Signature Authentication Service Provider towards Third Parties*." Bahrain Law Journal 3, no. 1 (2006): 304.
- Yassin, K. "*Determinants of the Cost of Liquidity in Emerging Markets and the Impact of the Global Credit Crisis*: An Analytical Study of Companies Listed on the Amman Stock Exchange for the Period (2003-2008)." PhD diss., Arab Academy for Banking and Financial Sciences, Amman, Jordan, 2010, 13.
- Younis, Arab. "*Electronic Banking Services"* . Dar Al-Fikr University, Alexandria, 2005, 12.

- Youssef, A., Z. M. Al-Senussi, M. N. Hanifa, and B. A. Barnes. "*Money Laundering Risks from the Perspective of Bankers and Regulators.*" In 7th International Conference on Financial Crime and Criminal Justice, Wadham College, Oxford, UK, 7. 2015.
- Zidane, Muhammad, and Hamo, Muhammad. "*Economic Insights."* 8 (June 2015): 161-181.

3. Legal Materials

1. **European Laws**

- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulation (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014, and (EU) No. 2016/1011
- Directive 93/13/EEC amended by Directive (EU) 2019/2161
- Article 8 of the European Electronic Signatures Directive (1999/93/EC)
- Directive (EU) 2015/2366 on payment services
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector
- Commission Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 on regulatory technical standards for strong client authentication
- Article 1(2) of Directive (EU) 2015/849 of the European Parliament and of the Council
- Article 32(3) of Directive (EU) 2015/849 of the European Parliament and of the Council
- Article 17 of Regulation 1093/2010 of the European Parliament and of the Council
- Article 25 of Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)

- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022, on digital operational resilience of the financial sector

- Article 17 of Regulation 1093/2010 of the European Parliament and of the Council

- Directive (EU) 2015/2366 on payment services

- Financial Supervision Act, 2002 (as amended 2014), Section 4.24a "Duty of Care"

- Financial Conduct Authority, Discussion Paper on Duty of Care and Potential Alternative Approaches DP18/5 (July 2018).

- Opinion Of The European Central Bank of 11 April 2022 on a proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (CON/2022/14).

2. Jordanian Laws:

- Jordanian Transactions Law No. (15) of 2015

- Jordanian Electronic Transactions Law No. 85/2001 published in the Official Gazette on 12/31/2001, Amended by Law No. 15 of 2015

- Article (25) of the Jordanian Transactions Law No. (15) of 2015

- Article (8) of the Jordanian Electronic Transactions Law No. 85 of 2001 Law 2, Jordanian Electronic Transactions Law No. 15 of 2015

- Law 2, Jordanian Electronic Transactions Law No. 15 of 2015

- Article (10/1) of the Saudi Transactions System

- Article (10/1) of the Saudi Transactions System

Jordanian Laws and Regulations:

- The Jordanian electronic payment and transfer system for funds 2017

- Law No. (46) of 2007 regarding the Anti-Money Laundering Law, amended by Law No. (31) 2015

- Article (2) of the Information Technology Crimes Law No. 27 of 2015 in Jordan

- Article 25 of the Jordanian Transactions Law of 2015

- Instructions for adapting to cyber risks issued by the Central Bank of Jordan for the year 2018

- Instructions issued by the Central Bank of Jordan regarding customer rights and duties 2022

- Technical requirements for electronic payment and transfer services companies issued by the Central Bank of Jordan 2018

- Application form for licensing electronic payment and transfer companies in the Hashemite Kingdom of Jordan issued by the Central Bank of Jordan for the year 2018

- Article 4 of the Central Bank of Jordan Law No. 23 of 1971

- Central Bank of Jordan, "Appendix (2/B): Indicators of Suspicion of Terrorist Financing Operations," 2018.

3. ***Books:***

- Plotkin, M., "*E-Commerce Law and Business",* "Aspen Publisher". United States of America, 2003.

- Trudell P., Abran F., Penikalf K., Heine S., "*Cyberspace Law, Montreal",* Themes Editions, 1997, p. 3

- Jacob A., "*Civil Liability of the Certification Service Provider",*2017 , p. 313

- Le Tourneau P, Number Contrats 2022/23 12ed - *Informatics and Reliable Electronics* , 2022, pp. 39

- Henry H. Perritt, Jr., "*Regulatory Models for Protecting Online Privacy*," Villanova University School of Law

- *David Garmon, "Information Security Policy Preparation Guide," SANS Institute*

- Wouter H. Muller, Christian H. Kalin, and John G. Goldsworth (Eds.), *Anti-Money Laundering: International Law and Practice,*2007, p 22.

- Sue Turner and Jonathan Bainbridge, "*Anti-Money Laundering Timeline and Stringent Regulatory Response,*" Criminal Law Journal,2018.

- J. Kremer, Y. A. de Montjoy, and H. Schweitzer, *Competition Policy in the Digital Age* (European Commission 2019).

- C. Sunstein, "*Risk and Cause: Safety, Law, and the Environment",* (CUP 2004)

- D, Bosch and C Van Dam (eds), "*The Bank's Duty of Care"* (Bloomsbury 2017).

- Scott, H., Gulliver J. and Nadler, H. "*Cloud Computing in the Financial Sector*", 2019, p12.

4. **Websites and Online Publications:**

- https://monzo.com/

- https://www.imf.org/en/Home

- Brun, M., The Nature and Implications of Certification in Internet Electronic Commerce, March 2000, https://www.lex-electronica.org/files/sites/103/7-1_brun.pdf (accessed January 25, 2023)

- Caprio E, European Directive, 13 December 1999, 1999 on a common module for electronic signature, GAS. Pal, October 2000, https://www.caprioli.ts.com/migration/pdf/signature_confiance_signelec.pdf (accessed January 27, 2023)

- European Banking Authority (2018). The text refers to Regulatory Technical Standards (RTS) relating to Strong Customer Authentication (SCA) and Common and Secure Communications (CSC) as set out in the Second Payment Services Directive (PSD2), https://www.eba.europa.eu/ (accessed October 17, 2023)

- Payment Card Industry Security Standards Council (PCI SSC) 2020. The current version of the PCI Data Security Standard (PCI DSS) is 4, https://www.pcisecuritystandards.org/ (accessed October 20, 2023)

- European Court of Justice ruling on banks' liability for unauthorized low-value transactions using contactless payment, Library of Congress (December 21, 2020)

- https://www.ntia.gov/

- https://www.bis.org/cpmi/publ/d187.pdf

- https://cutt.us/NqO3S

- https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/27/06/Fintech-The-Experience-So-Far-47056

- https://www.bis.org/bcbs/publ/d486.htm

- https://www.bis.org/publ/cpss101a.pdf

-https://www.bruegel.org/2018/10/a-better-european-union-architecture-to-fight-money-laundering/

- https://cutt.us/prtVt

- https://www.cbj.gov.jo/Default.aspx

- https://2u.pw/vKWNHH0w

- https://2u.pw/xpk5vs3P

- https://2u.pw/yvlzpKUY

- https://2u.pw/gCg0De1X

- https://2u.pw/YekDgXMY

5. Reports and Studies:

- Article 11 UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001

- Article 6 UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001

- Jordan’s National Payments System Report 2021 issued by the Central Bank of Jordan

- Jordan’s National Payments System Report 2021 issued by the Central Bank of Jordan

- Study on Consumer Payments in the Euro Area (SPACE), 2022 by the European Central Bank

- UNCITRAL Trade Law Promoting Trust in Electronic Commerce: Legal Issues Relating to the International Use of Electronic Authentication and Signature Methods, United Nations, Vienna

- The annual report of the payment system in Jordan issued by the Central Bank of Jordan for the year 2022

- Department of Economic and Social Affairs, United Nations Guidelines for Consumer Protection (as expanded in 1999), United Nations, New York, 2003

- EBA (2021e), Report on the use of digital platforms in the EU banking and payments sector, EBA/REP/2021/26, September

- EIOPA (2020b), Discussion paper on (re)insurance value chain and new business models

- EBA (2021d), EBA Analysis of Regulatory Technology in the EU Financial Sector, EBA/REP/2021/17, June

- EIOPA (2021b), Discussion Paper on Blockchain and Smart Contracts

- Anderberg, A. et al. (2019), Blockchain Now and Tomorrow: Assessing the Multidimensional Impacts of Distributed Ledger Technologies, Publications Office of the European Union

- IDC and Statista (2021), Volume of data/information created, captured, copied and consumed worldwide from 2010 to 2025 (in zettabytes), graph, June 7

- EBA (2020c), EBA Report on Big Data and Advanced Analytics, EBA/REP/2020/01, January

- EIOPA (2019b), Big Data Analytics in Auto and Health Insurance: A Thematic Review

- Financial Stability Board (2019a), FinTech and Market Structure in Financial Services: Market Developments and Potential Implications for Financial Stability, 14 February

- Joint Committee of European Service Unions (2018), Joint Committee Report on the Outcomes of the Monitoring Process on 'Automation in Financial Advice', JC 2018-29, 5 September

- McKinsey Global Institute (2021), Unrestricted Financial Data: The Value of Open Data for Individuals and Organizations, Discussion Paper, June

- European Commission communications and fact sheet issued on 19 February 2020, available at: European Data Strategy

- ECB Working Paper Series No. 223, 22 May 2019

- Review of Directive (EU) 2015/2366 on payment services

- Central Bank of Jordan, National System Review and Monitoring Department, Sixth Report, 2021.

- GSM Association (2016) "Mobile Money Protection: How Services and Systems Can Ensure Customer Protection"

- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001

- Financial Action Task Force (2013) "Guidance for a risk-based approach to prepaid cards, mobile payments and online payment services"

- Financial Action Task Force (2019) "Guidance for a risk-based approach to virtual assets and virtual asset service providers"

- Basel Committee on Banking Supervision (2019) "Report on open banking and APIs"

- Committee on Payments and Market Infrastructure and International Organization of Securities Commissions (2016) "Cyber Resilience Guidance for Financial Market Infrastructure"

- Department of Economic and Social Affairs, United Nations Guidelines for Consumer Protection (as expanded in 1999), United Nations, New York, 2003

- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001

- Financial Action Task Force (2013) "Guidance for a risk-based approach to prepaid cards, mobile payments and online payment services"

- Financial Action Task Force (2019) "Guidance for a risk-based approach to virtual assets and virtual asset service providers"

- Basel Committee on Banking Supervision (2019) “Report on open banking and APIs”

- Committee on Payments and Market Infrastructure and International Organization of Securities Commissions (2016) “Cyber Resilience Guidance for Financial Market Infrastructure”

- Central Bank of Jordan, National Payments System Oversight Department, Sixth Annual Report, 2021

- G7 (2019) “Investigating the impact of global stablecoins”

- Joint QR Code Standards Guide for Payments in Jordan, JOPACC, 2022

- European Central Bank (ECB) Occasional Paper Series No. 223/22 May 2019

- IMF and World Bank (2019) “FinTech: Experience to Date”, IMF Policy Paper

- The National Strategy for Electronic Payments in Jordan (2023-2025) issued by the Central Bank of Jordan

- Digital signature and authentication certificate: concept and legal implications, “Al-Manara Magazine - Al-Bayt University.” Vol. 11, No. 4, p. 249, 2005

- Development of Evidence and Electronic Evidence, “American Bar Association Publications.” 2008, p. 11

- Effects of technology-based innovation on financial performance of listed commercial banks in Ethiopia: The case of electronic banking. Turkish online journal of qualitative inquiry. 2021, Volume 12, Issue 8, p. 6687

−"Digital Signature and Certificate of Authenticity: Concept and Legal Implications." Al-Manara Magazine - Al-Bayt University, 2005, vol. 11, No. 4, p. 249. United Nations Publications, 2009. http://uncitral.org/uncitral/en/publications/publications.html.