Dr. Sherif Mohsen Abdelfattah Shaltout

Instructor, General Manager, Audit, Banque Du Caire

The Adoption of Open Banking Concept to Regulate Arab Countries Digital Payment

Correspondence:

Dr. Sherif Mohsen Abdelfattah Shaltout, Instructor, General Manager, Audit, Banque Du Caire.

DOI: https://doi.org/10.54873/jolets.v3i2.146

E-mail: sshltoot@nu.edu.eg

Citation:

Sherif Mohsen AbdelFattah Shaltout, The Adoption of Open Banking Concept to Regulate Arab Countries Digital Payment, Conference Research Papers The Third International Conference on Legal Aspects of Digital Transformation: Opportunities and Challenges, Faculty of Law at British University in Egypt, Cairo 17-18 June 2023, Journal of Law and Emerging Technologies, Volume 3, Issue 2, October 2023, p. 47-98

The Adoption of Open Banking Concept to Regulate Arab Countries Digital Payment

Dr. Sherif Mohsen Abdelfattah Shaltout

Abstract:

The emergence of fintech has disrupted the traditional banking landscape, challenging the notion that banks are the sole providers of financial services. In the past, entrepreneurs were often seen as disruptors to traditional banking models. However, banks have now recognized the value of collaborating with fintech companies to expand the range and accessibility of financial products and services for customers. The payment industry has become a focal point for banks and fintech startups, with the proliferation of new payment options, such as mobile payments.

By leveraging fintech advancements, banks can offer diverse payment solutions to customers without having to develop them in-house. This study examines the current regulatory landscape of payment systems, identifies existing payment governance practices, and proposes recommendations to enhance the digital payment environment in Arab countries while addressing significant regulatory concerns.

Understanding the evolving relationship between banks and fintech firms, as well as the regulatory considerations surrounding digital payments, is crucial for industry participants, policymakers, and regulators. By exploring these topics, this study aims to provide valuable insights and guidance for navigating the changing payment landscape effectively and fostering a robust digital payment ecosystem in Arab countries.

Through this examination, the study intends to contribute valuable guidance for Arab countries in developing a robust and regulated digital payment ecosystem, fostering financial inclusion, and promoting innovation in the region.

Keywords: Payment Services Directive Ver.2 – Open banking - Service Level Agreement –Operational Level Agreement - Underpinning Contract - payment Service Operator.

استخدام مفهوم الانفتاح المصرفي لإحكام الرقابة وتنظيم المدفوعات الرقمية في الدول العربية

د. شريف محسن عبد الفتاح شلتوت

رئيس قطاع مراجعة نظم المعلومات، بنك القاهرة

الملخص:

أدى ظهور التكنولوجيا المالية إلى إحداث تحول ملحوظ في كيفية أداء الخدمات المصرفية، لتتجاوز الفكرة السائدة التي تتبنى فكرة أن البنوك هي المزود الوحيد للخدمات المالية. حيث إنه في الماضي، كان يُنظر إلى رواد الأعمال على أنهم معطلون للنماذج المصرفية التقليدية إلا أنه في الأونة الأخيرة أدركت البنوك قيمة التعاون مع شركات التكنولوجيا المالية لتوسيع نطاق المنتجات والخدمات المالية وسهولة الوصول إليها للعملاء. فقد أصبحت صناعة المدفوعات محط اهتمام البنوك وشركات التكنولوجيا المالية الناشئة، مع انتشار خيارات دفع جديدة، مثل الدفع عبر الهاتف المحمول.

فيمكن للبنوك من خلال الاستفادة من التقدم في مجال التكنولوجيا المالية تقديم حلول دفع متنوعة للعملاء دون الحاجة إلى تطويرها داخليًا. لذا تقوم هذه الدراسة على التعرف على المشهد التنظيمي الحالي لأنظمة الدفع، وتحديد ممارسات حوكمة المدفوعات الحالية، وتقديم توصيات لتعزيز بيئة الدفع الرقمي في الدول العربية مع معالجة المخاوف التنظيمية الرئيسية.

فقد بات من الضروري فهم العلاقة المتطورة بين البنوك وشركات التكنولوجيا المالية، بالإضافة إلى الاعتبارات التنظيمية المحيطة بالمدفوعات الرقمية، للمشاركين في الصناعة وصانعي السياسات والمنظمين. من خلال استكشاف هذه الموضوعات، تهدف هذه الدراسة إلى تقديم رؤى وإرشادات قيمة للتنقل في مشهد الدفع المتغير بشكل فعال وتعزيز نظام دفع رقمي قوي في الدول العربية.

من خلال هذا العرض، تهدف هذه الدراسة أيضا إلى تقديم إرشادات قيمة للدول العربية في تطوير نظام دفع رقمي قوي ومنظم، وتعزيز الشمول المالية بالإضافة إلى تشجيع الابتكار في المنطقة.

الكلمات الرئيسية: توجيه خدمات الدفع الإصدار – الانفتاح المصرفي – اتفاقية مستوى الخدمة – اتفاقية المستوى التشغيلي – العقد الأساسي – مشغل خدمة الدفع.

List of Abbreviations

Abbreviation	Definition
PSD2	Payment Services Directive Ver.2
KSA	Kingdom of Saudi Arabia
UAE	United Arab Emirates
SLA	Service Level Agreement
OLA	Operational Level Agreement
UC	Underpinning Contract
PSO	Payment Service Operator
PSP	Payment Service Provider
eKYC	Electronic Know Your Customer
BaaS	Banking as a Service
API	Application Program Interface
SaaS	Software as a Service
AML	Anti-Money Laundry
CBE	Central Bank of Egypt
SAMA	Saudi Arabian Monetary Agency
FRA	Financial Regulatory Association
FinTech	Financial Technology
FMI	Financial Market Infrastructure
FATF	Financial Action Task Force

1. Introduction

The fin-tech ecosystem has been broken down by Haddad and Hornuf into nine major groups. In the first class of businesses known as asset management, fintech companies offer services including robo-advice, social trading, wealth management, and software or apps for managing personal finances. Startups that provide stock exchange or financial services, such as trading stocks, derivatives, and other financial products, fall under the second category, exchange services. The third sector is finance, which comprises businesses that offer crowdsourcing, crowdlending, microcredit, and factoring services. The fourth sector is insurance, which comprises companies providing services like usage-driven insurance brokerage, peer-to-peer insurance, spot insurance, brokerage services, management of insurance contracts, claims, and risk management services. Loyalty programmers make up the fifth group. These startups provide clients with loyalty program services while usually utilizing big data. The sixth category includes other fintech startups that offer investor education and training, innovative background services (like authorization services or near-field communication systems), white-label solutions for various business models, or other technological advancements falling under other business activities. The seventh category, which is devoted to business models that offer novel and innovative payment solutions, is focused on payment systems, such as mobile payment systems, e-wallets, or cryptocurrencies. The banking industry can benefit from services provided by fintech companies that employ technology to streamline regulatory monitoring, reporting, and compliance in the eighth market segment, which is referred to as regulatory technology. The ninth area, risk management, covers companies that help businesses assess the financial reliability of their counterparties or enhance their own risk management practices [(1)].

(1) Hornuf, C. H. The emergence of the global fintech market: economic and technological determinants. Retrieved from https://www.researchgate.net/publication/324050315_The_emergence_of_the_global_fintech_market_economic_and_technological_determinants. 2018.

According to the categories listed above, it is crucial to have a regulatory framework that effectively controls digital payment systems while simultaneously ensuring consumer safety, fostering innovation, and increasing financial inclusion as the Arab world embraces the digital age. The potential to modify Payment Services Directive 2 (PSD2) to meet the unique needs of the Arab market presents the opportunity to enhance the regulatory environment and create a more secure and efficient financial ecosystem.

The financial environment has seen substantial change over time, with each Fintech era bringing new innovations and challenges. The interaction between traditional financial institutions and fintech businesses is challenging. In order to increase the scope and volume of their financial services and products, banks have learned the benefit of working with fintech companies, despite the fact that many startups were first seen as competitors to traditional banking models.

Payment systems, financial market infrastructures (FMIs), and digital financial services (DFS) all contribute to financial stability, economic growth, and financial inclusion. As a result, developing secure, dependable, and effective domestic and international payment systems as well as FMIs is a crucial part of the World Bank Group's (WBG) efforts to combat poverty and promote shared prosperity [1] The payment sector has evolved into one of the key areas of collaboration between banks and fintech companies as a result of the introduction of new payment methods like mobile payments. Banks rely on fintech expertise to advance these payment technologies and offer them to their clients since internal development is not necessary. Another significant area for cooperation is lending, where banks may team up with fintech to provide customers with specialized banking information tailored to

(1) World Bank. The World Bank. Retrieved from Payment Systems: https://www.worldbank.org/en/topic/paymentsystemsremittances#:~:text=Payment%20%26%20settlement%20systems%20are%20mechanisms,and%20help%20expand%20financial%20inclusion. 2022.

their particular need. Despite challenges such cultural differences, regulatory compliance, integration issues, and issues with intellectual property, the relationship between banks and fintech startups continues to grow; more collaborations are expected in the future [(1)].

Banks and Fintech companies have a dynamic relationship that has been marked by both cooperation and disruption. Many startups were initially viewed as disruptors that posed a threat to the incumbent banking industry. But as time has gone on, banks have realized the value of collaborating with fintech firms to broaden their selection of banking goods and services. This collaboration is especially evident in the payments sector, where banks have used fintech know-how to create cutting-edge payment options like mobile payment systems. Another crucial area for collaboration between banks and fintech companies is lending, where services may be tailored to specific customer preferences. Despite barriers brought on by cultural differences, regulatory compliance, integration, and intellectual property, it is anticipated that the relationship between banks and fintech startups will continue to grow[(2)].

As a result of its accessibility, speed, and convenience, digital payment systems have grown in popularity. However, as digital payments become more widely used, a suitable regulatory framework is also needed to handle risks, safeguard customers, and guarantee a safe and effective financial ecosystem. The Payment Services Directive 2 (PSD2), which was implemented in the European Union, has been successful in fostering competition, innovation, and consumer rights in the market for digital payments. By enabling

(1) Thomsett, L. W. The Digital Banking Revolution. Deutche Nationalbibliografie. Retrieved from https://books.google.com.eg/books?hl=en&lr=&id=YDrEDwAAQBAJ&oi=fnd&pg=PR7&dq=The+financial+landscape+has+undergone+significant+transformations+throughout+history,+with+each+era+of+Fintech+bringing+unique+advancements+and+challenges.+Fintech+firms+have+had. 2019.

(2) Welcome Sibanda, E. N.. Digital technology disruption on bank business models. International Journal of Business performance Managment. Retrieved from https://www.inderscienceonline.com/doi/abs/10.1504/IJBPM.2020.106121. March 30, 2020.

open banking and allowing third-party providers access to client account information and payment initiation services, PSD2 has encouraged the launch of new payment services, improved user experiences, and increased market competition. (PSD2) has significantly changed the financial environment within the European Union (EU). PSD2 has paved the way for a more vibrant and client-focused financial ecosystem by increasing consumer protection, supporting innovation, and boosting competition in payment services. The Payment Services Directive 2 (PSD2) has had a significant impact on the financial landscape in the European Union by fostering innovation, enhancing consumer protection, and fostering competition in the payment services sector. Due to PSD2's success in Europe, there is rising interest in changing PSD2's regulatory framework for payment systems in Arab countries. The financial climate in the European Union (EU) has undergone a considerable transformation as a result of (PSD2). By enhancing consumer protection, encouraging innovation, and fostering greater competition in the payment services industry, PSD2 has prepared the road for a more vibrant and customer-focused financial environment [(1)].

The suitability of PSD2 for Arab countries, recommendations for necessary modifications, or insights into potential challenges and risks that need to be addressed during implementation are not covered in depth by this study, nor will it include an analysis of a mixed-methods approach that combines qualitative analysis of regulatory frameworks and market dynamics with quantitative evaluations of consumer behavior and technological infrastructure. This study examines the potential advantages of enacting PSD2-inspired legislation in Arab countries while taking into account the region's unique cultural, economic, and legal features. By carefully comparing the current state of the payment systems and legal frameworks in Arab countries, this study seeks

(1) Impact of PSD2 on The Payment Services Market. Retrieved from sciendo: https://sciendo.com/article/10.2478/wrlae-2021-0008. October 26, 2021.

to identify the key areas that require improvement. Its sole purpose is to introduce legal concepts related to open banking, payment systems, digital identities, and other digital payment procedures. Future research in this area should provide a comprehensive assessment of the legal implications and potential repercussions on payment systems, cybersecurity, data privacy, competition, and financial inclusion. In order to foster effective, secure, and cutting-edge payment ecosystems while ensuring consumer protection and market stability, this study aims to inform policymakers, regulators, financial institutions, and industry participants about the opportunities and challenges of adopting PSD2-inspired regulations in Arab countries.

This research has produced useful insights for policymakers by reviewing the current legal framework, identifying existing governance practices, and analyzing the implications of digital payment developments. The conclusion emphasizes the necessity of fostering a regulatory environment that encourages innovation, protects consumer interests, and accelerates the expansion of digital payments. If followed, these proposals will help to the overall development of the financial sector, improve financial inclusion, and assist the region's economic progress in the digital era by promoting a dynamic and secure digital payment ecosystem

2. Research Scope and Objectives

FinTech can be broadly characterized as technological advancements that enhance how funds are transmitted, raised, and invested. The Researcher will thus take a close look at each of these three market areas in a further separate document, analyze the technological and commercial aspects of their advances, and demonstrate how each of them may be effectively regulated. However, this document addresses only the regulation of digital payment solutions which is apart from fund transmission where other methods will be covered in a further publication.

2.1 Research Scope

FinTech can be broadly characterized as technological advancements that enhance how funds are transmitted, raised, and invested. This document covers payment innovations that do not rely on decentralized technologies, such as blockchain. A good example of this type of innovation is the digital and mobile wallet, for instance, PayPal, Venmo, and Apple and Android Pay. We first looked at the Evolution of Open Banking concept and the supported regulations by mentioning the growth of Banking as a service concept BaaS followed by Updated digital Payment executive regulation in Both KSA and UAE followed by Evolving Landscape of Digital Banking Methods and Stakeholders and afterwards we exposed the Differentiation between UC, SLA, and OLA Agreements in the Financial Industry. We explained PSD2 and Open Banking: Implications, Challenges, and its adaption in Egypt's Payment. After that we highlighted the Significance of Digital Identity in Banking and eKYC Processes. We end up in this section with the explanation of the current Regulation of Digital Identity and Digital Payment.

The Researcher will thus take a close look at each of these three market areas in a separate document, analyze the technological and commercial aspects of their advances, and demonstrate how each of them may be effectively regulated.

Therefore, this document provides an in-depth analysis of payment innovations that do not rely on decentralized technologies like blockchain. It focuses on various advancements in digital payments and explores their technological and commercial aspects, as well as the necessary regulations for their effective implementation. The scope of this document encompasses the following topics:

1. Evolution of Open Banking Concept and Supported Regulations:

- The document delves into the concept of Open Banking and its evolution over time.
- It highlights the regulatory framework that supports Open Banking, including the growth of Banking as a Service (BaaS) concept.
- The researcher discusses the updated digital payment executive regulations in both the Kingdom of Saudi Arabia (KSA) and the United Arab Emirates (UAE).

2. Evolving Landscape of Digital Banking Methods and Stakeholders:

- This section explores the changing landscape of digital banking methods, including the emergence of digital and mobile wallets.
- Prominent digital wallet platforms such as PayPal, Venmo, Apple Pay, and Android Pay are discussed as examples of innovative payment solutions.
- The document analyzes the various stakeholders involved in the digital banking ecosystem, including financial institutions, technology providers, and regulatory bodies.

3. Differentiation between UC, SLA, and OLA Agreements in the Financial Industry:

- The researcher provides an explanation of the distinctions between Underwriting Agreement (UC), Service Level Agreement (SLA), and Operational Level Agreement (OLA) in the financial industry.
- The document outlines the roles and responsibilities of each agreement type and their significance in ensuring smooth financial operations.

4. **Implications and Challenges of PSD2 and Open Banking in Egypt's Payment System:**
   - This section focuses on the implications and challenges of the Revised Payment Services Directive (PSD2) and Open Banking in Egypt's payment landscape.
   - The researcher highlights the potential benefits and risks associated with these regulatory frameworks and their impact on the country's financial ecosystem.
5. **Significance of Digital Identity in Banking and eKYC Processes:**
   - The document emphasizes the importance of digital identity in the banking sector, particularly in the context of electronic Know Your Customer (eKYC) processes.
   - It discusses the role of digital identity verification in enhancing security, improving customer experience, and facilitating seamless digital transactions.
6. **Regulatory Approaches for Digital Identity and Digital Payment FinTech:**
   - The final section explores different regulatory approaches to digital identity and digital payment FinTech.
   - The researcher provides insights into effective regulatory measures that can ensure consumer protection, data privacy, and financial stability in the rapidly evolving FinTech landscape.
   - By examining each of these topics individually, the document aims to provide a comprehensive understanding of non-blockchain payment innovations and the regulatory considerations associated with them.

2.2 Research Objectives

This document provides a comprehensive analysis of non-blockchain payment innovations and the regulatory considerations associated with them. It examines the evolution of Open Banking, digital payment regulations, the evolving landscape of digital banking methods, financial agreements, implications of PSD2 and Open Banking in Egypt, the significance of digital identity in banking, and regulatory approaches for digital identity and payment FinTech. Understanding these advancements and regulatory measures is crucial for industry participants, policymakers, and regulators to navigate the changing payment landscape effectively. this document provides a comprehensive analysis of non-blockchain payment innovations and the regulatory considerations associated with them. It examines the evolution of Open Banking, digital payment regulations, the evolving landscape of digital banking methods, financial agreements, implications of PSD2 and Open Banking in Egypt, the significance of digital identity in banking, and regulatory approaches for digital identity and payment FinTech. Understanding these advancements and regulatory measures is crucial for industry participants, policymakers, and regulators to navigate the changing payment landscape effectively.

3. Evolution of Open Banking concept and the supported regulations

The concept of Open Banking has evolved over time, transforming the banking industry. This evolution has been supported by a regulatory framework that promotes innovation and competition. Open Banking enables the sharing of financial data and services through secure APIs, leading to increased customer control and enhanced financial experiences. Regulatory measures have been implemented to ensure data privacy, security, and consumer protection in this evolving landscape.

3.1 Growth of the BaaS concept

Independent APIs will eventually be produced via open banking. A comparable change is also something we expect to see in non-banking industries, including insurance, travel, logistics, and communication (1). It is anticipated that these sectors will offer additional APIs that can be re-bundled to represent different segments of sectors other than financial services. By combining health and financial data and integrating health and financial data APIs, this may be proven. Banks can then provide customers with individualized financial advice based on their health state or by combining financial APIs with social media data APIs. For instance, the bank may recommend travel-reward credit cards or savings accounts to a customer who frequently tweets about travel. All of this will combine to offer highly specific banking solutions that are personally personalized and far more appealing to a tiny niche set of end clients.

These industries are expected to provide more APIs that can be re-bundled to represent elements of industries other than financial services. This can be demonstrated by combining social media data APIs with financial APIs to create a single health and financial data API, or by integrating health and financial APIs so that banks can offer customers individualized financial advice based on their health status [(2)].

In other words, the delivery of BaaS is comparable to that of SaaS in that the contract allowing the right to direct access to the flow of those services plays the part of the business capital that would ordinarily support the supply of banking services. A BaaS arrangement permits a non-financial organization to act as the buyer while allowing a licensed bank to handle the delivery of banking services. The authorized bank then funds the non-

(1) Dize Dinckol, P. O.. egulatory standards and consequences for industry architecture: The case of UK Open Banking. ELSEVIER. 2023.

(2) Omarini, A.. Unbundling and re-bundling in the open industry of banking. Routledge. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9780429292903-15/fintechs-anna-omarini. 2021.

financial firm's client-related business transactions. BaaS improves consumer network accessibility by enabling non-banks to provide financial services to their customers using a limited context-based distribution strategy [(1)].

Customers can have quick, safe access to cutting-edge financial solutions thanks to open banking. Customers can still transact business with their bank while using one or more financial products provided by a third party. Because consumers aren't providing their banking login information to outside service providers when they use screen scraping, security and liability problems are also reduced [(2)]. Open banking lowers the cost of obtaining financial products from third-party providers and boosts competition in the financial sector by enabling fintech businesses and financial institutions to offer new services and products to a larger customer base [(3)]. By giving people the opportunity to integrate their financial data and making it possible for them to manage their finances more effectively, especially for geographically dispersed individuals and underprivileged groups, it can also have a revolutionary impact on society[(4)].

The recommendations should be modified and tailored to fit the specific legal, regulatory, and economic circumstances that may exist in each Arab country. Collaboration between Arab nations could be beneficial for information sharing and coordinating regional regulatory frameworks for open banking. A legislative framework that encourages secure data sharing, collaboration, and customer-centric financial services banking has the potential to revolutionise industries, as shown by the European experience with PSD2

(1) Resano. 2021.
(2) Markos Zachariadis, P. O..The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199. 2017.
(3) Thomsett, L. W.. The Digital Banking Revolution. Deutche Nationalbibliografie. Retrieved from https://books.google.com.eg/books?hl=en&lr=&id=YDrEDwAAQBAJ&oi=fnd&pg=PR7&dq=The+financial+landscape+has+undergone+significant+transformations+throughout+history,+with+each+era+of+Fintech+bringing+unique+advancements+and+challenges.+Fintech+firms+have+had. 2019.
(4) Thomas Walker. 2023.

and open banking [1]. By applying the knowledge gained from these findings to the design and implementation of their own open banking frameworks while taking into account their distinct legal, regulatory, and economic contexts, Arab countries can benefit from increased competition, innovation, financial inclusion, and consumer empowerment in their respective financial systems. Both parties should seek legal advice to ensure that the API contract is comprehensive, consistent with their business objectives, and protects their interests while creating win-win cooperation.

The technical requirements for an API contract should outline the parties' respective obligations, liabilities, and rights to access and use the data. This determines how the interaction between banks and fintech companies will be set up. These circumstances are: Data Access and Usage is the first section, where it should be made clear exactly what kinds of data the fintech company can access and use through the bank's systems [2]: Why they are important and how to get them effectively, 2023), as well as any limitations on sharing or commercialization. Technical details: To outline the technical requirements, policies, and procedures required to interface the fintech company's systems with the bank's API. Data formats, security measures, authentication methods, API versioning, error handling, and accessibility rules are all covered in this. The final section talks about privacy and security issues. The security precautions, data encryption methods, access limitations, and incident response processes that must be followed by all parties are outlined in this paper. It should be made clear whether the website conforms with applicable data protection and privacy laws, such as GDPR [3]. Service level agreements (SLAs) are the fourth. The level of performance and service that may be

(1) Dize Dinckol, P. O. egulatory standards and consequences for industry architecture: The case of UK Open Banking. ELSEVIER. 2023.
(2) API agreements: Why they matter & how to get them right. Retrieved from michalsons: https://www.michalsons.com/blog/api-agreements-why-they-matter-how-to-get-them-right/65117. April 12, 2023.
(3) Michon, M. Understanding an API provider's privacy policy. Retrieved from Bearer : https://www.bearer.com/blog/understanding-an-api-providers-privacy-policy. April 22, 2023.

expected from each party is defined by these SLAs, which are important. As well as any penalties or remedies for non-compliance, the agreement should include KPIs like uptime, response times, and support availability [1]. Fifth: The right to intellectual property All intellectual property, such as software, APIs, documentation, and any breakthroughs or advancements achieved during the collaboration, should be clearly defined in the contract with regard to ownership and usage rights. If any licenses or royalties are necessary for the usage of proprietary technology, that information should be included as well. The sixth is liability and indemnity. The agreement should specify who is responsible for any violations, losses, or damages incurred throughout the collaboration. Theresa M. Weisenberger [2] argues that indemnity clauses, dispute resolution procedures, and financial responsibilities in the event of security events, data breaches, or contract violations should all be included. Termination provisions that outline the circumstances under which each party may end the agreement should be included in the contract. We wish to discuss termination and exit plans as our seventh point. Laying out the procedures for data transfer, system decommissioning, and any transition support necessary upon contract termination or expiration is suggested in the paper Exit Planning for Microsoft Cloud Services [3], 2020. All applicable regulations, including those governing financial transactions, data security, anti-money laundering (AML), and know your customer (KYC) requirements, must be complied with in accordance with the terms of the agreement. It should be understood that both parties will uphold their legal responsibilities and cooperate with any audits or regulatory inspections that may be carried out. The contract should include a governance framework outlining roles and responsibilities,

(1) Simpson, J. How to Set SLAs for Cloud APIs. Retrieved from NORDIC: https://nordicapis.com/how-to-set-slas-for-cloud-apis/. September 27, 2022.
(2) Theresa M. Weisenberger. Application Programming Interfaces (APIs). LexixNexis/ Practical Guidance , 3 4. 2022.
(3) Exit Planning for Microsoft Cloud Services. Retrieved from microsoft.com: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWBkvx. August, 2020.

communication channels, escalation procedures, and regular review methods in order to manage the ongoing relationship between the fintech company and the bank.

BaaS, which is expanding as a result of partnerships between conventional banks and fintech companies, has an impact on both sides (from both the right and left views). In terms of the right perspective, the appropriate viewpoint considers three factors: First Competition and innovation. The advent of BaaS and fintech promotes healthy competition in the banking sector. By offering cutting-edge tools and solutions, fintech companies can put pressure on traditional banks to improve their offerings and customer service [(1)]. Second: Access to Financial Services: By giving underserved people access to banking services, fintech firms and BaaS platforms promote financial inclusion. Through digital technology, they can interact with unbanked people and provide them with practical and inexpensive financial solutions. Efficiency and cost-cutting are prioritized [(2)]. third. Traditional banks can increase operational efficiency by utilising the infrastructure and know-how of fintech companies through BaaS agreements. As a result, banks might experience cost savings that would allow them to use their resources more carefully [(3)]20. For instance, the Egyptian fintech business Fawry Pay provides banks with BaaS solutions in the Egyptian market (right viewpoint). To facilitate client transactions and provide digital payment services, partner banks must provide payment infrastructure. With the help of Fawry Pay's platform, banks can utilize mobile payments, digital wallets, and other cutting-edge technology.

On the other hand, the left perspective takes into account two important

(1) Innovation through BaaS and embedded finance. Retrieved from Finntech Futures: https://www.fintechfutures.com/2023/05/innovation-through-baas-and-embedded-finance/. 2023.

(2) World Bank. Fintech and Financial Services: Delivering for development. Retrieved from World Bank Blogs: https://blogs.worldbank.org/voices/fintech-and-financial-services-delivering-development. February 24, 2023.

(3) FinnTech Magazine. How BaaS unlocks vast opportunities for the banking sector. Retrieved from FinnTech Magazine: https://fintechmagazine.com/articles/how-baas-unlocks-vast-opportunities-for-the-banking-sector. February 12, 2023.

factors: First off, challenges with risk management and regulatory compliance arise as a result of fintech's disruption of traditional banks. As a result, risks like cybersecurity breaches or operational breakdowns may exist for both clients and the financial system. The regulatory oversight and capital requirements that apply to traditional banks may not apply to fintech companies [(1)]. Second, consumer protection may encounter challenges as BaaS and fintech develop. Customers may be exposed to unfair practices or insufficient dispute resolution procedures since fintech companies do not follow the same consumer protection requirements as traditional banks [(2)]22.

Both tactics are appropriate for the Egyptian market. Innovative payment methods created by fintech businesses like Fawry Pay and Bee have increased access to financial services. To ensure a safe and open financial system, it is essential to maintain a balance between competition and innovation, risk management, consumer protection, and legal compliance. In order to protect consumer interests and ensure financial stability, regulatory agencies in Egypt, such as the Central Bank of Egypt (CBE) and the Financial Regulatory Association (FRA), are in charge of monitoring and controlling fintech operations.

3.2 Updated digital Payment executive regulation in Both KSA and UAE

In banking practices, the terms «payment service» and «payment system» are frequently used synonymously to refer to the same concept. However, as will be discussed later, they are actually distinct terms. The term «payment service» refers to a range of services related to fund transfer transactions carried out with or without the use of payment accounts, including the operation of payment accounts (such as cash deposits or withdrawals), the

(1) Li, G. Fintech, Bank Risk-Taking, and Risk-Warning for Commercial Banks in the Era of Digital Technology. Retrieved from https://doi.org/10.3389/fpsyg.2022.934053. July 22, 2022.
(2) Federal Reserve Bank Of ST.LOUIS. Consumer Protection in the Fintech Era. Retrieved from https://www.stlouisfed.org/en/on-the-economy/2021/march/consumer-protection-fintech-era. March 28, 2021.

issuance or acceptance of payment instruments (such as debit cards), and mobile payments. Payment service users receive these services from the provider of the payment service. For instance, all services that the banks offer when a consumer transfers money from one bank account to another fall under the category of payment services. In this instance, the client is the one who benefits from the service, and the banks are the ones who supply the payment services. On the other hand, the term «payment system» refers to the unique setup utilized for interbank cash transfers. For Example, Interbank transfers in Turkey are carried out using the Electronic Fund Transfer (EFT) System, a payment platform run by the CBRT. This technology enables interbank transactions as well as the safe and quick transmission of payments between customers of various institutions [(1)].

Highlighting the similarities, variations, and major features of each regulatory framework in order to shed light on the introduction of the executive regulations on digital payments issued by the central banks of Saudi Arabia and the UAE. The United Arab Emirates (UAE) and Saudi Arabia's central banks have both released executive orders to control digital payments within their respective countries. This study attempts to offer a thorough and comparative examination of the executive regulations concerning digital payments published by the central banks of Saudi Arabia and the United Arab Emirates.

Following a statement issued by the Saudi Central Bank (SAMA) on April 7, a draught executive regulation of the Payments and Payment Services Law has been made available for public feedback. Through the National Competitiveness Centre's public consultation portal (Istitlaa), the central bank invited comments and recommendations on the matter from interested

(1) CTMB, T. C. System, Payment Service and Payment. Retrieved from TCMB: https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/Payment+Service+and+Payment+System/#:~:text=In%20this%20case%2C%20the%20banks,used%20for%20interbank%20money%20transfers. 2023.

parties and members of the general public. Articles 7 and 18 of the Payments and Payment Services Law grant the SAMA regulatory powers, including the authority to publish the rule. The implementing legislation seeks to encourage adherence to pertinent international norms and principles in order to ensure that SAMA can exercise its jurisdiction [1]. The comments on the draught regulations must be submitted within 20 days, and they will be taken into account once the regulations are written. Specific executive rules, laws, directives, and specifications are included in this framework. These laws control several facets of electronic payments, including the licensing and authorization procedures for service providers. The central bank's official publication [2] lists the date these regulations were issued.

Similar to this, the central bank of the UAE has put in place its own set of executive rules to control electronic payments. These rules include pertinent laws, rules, and directives that are suited to the particular requirements of the digital payment environment in the UAE. The UAE Central Bank's Regulatory Framework for Stored Values and Electronic Payment Systems (the Regulation) is an essential piece of law that recognizes the importance of and regulates this swiftly growing market. It aspires to create a safe and secure environment for digital payment services with a focus on safeguarding customers and supporting innovation and competition in order to promote banking modernization and financial inclusion. Each of the four categories of payment service providers (PSPs) identified in the Regulation must get a license from the Central Bank in order to provide digital payment services in the United Arab Emirates: The retail PSP offers money transfers in addition to retail, governmental, and peer-to-peer digital payment services, much like a commercial bank would.

(1) SAMA issues draft regulation of payments law for public consultation. Retrieved from Argaam: https://www.argaam.com/en/article/articledetail/id/1550402. April 7, 2022.
(2) SAMA issues draft regulation of payments law for public consultation. Retrieved from Argaam: https://www.argaam.com/en/article/articledetail/id/1550402. April 7, 2022.

The official federal and local government entities that offer government digital payment services are included in the government PSP[1]. The non-issuing PSP is a non-deposit-taking organization that offers retail, governmental, and peer-to-peer services even though it does not issue digital currency itself.

3.3. Evolving Landscape of Digital Banking Methods and Stakeholders

Throughout history, payment systems have undergone significant changes. Previously, these systems involved three main parties: the drawer, the drawee, and the beneficiary. However, the rise of technology has revolutionized the payment landscape, introducing new stakeholders and methods. Today, digital payment systems encompass a wide range of participants, including merchants, acquirers, payment service providers (PSPs), payment service directives (PSDs), facilitators, and aggregators.

As e-commerce and electronic payments gained momentum, the inclusion of additional parties became necessary. Merchants were integrated into the system, facilitating online transactions. Acquirers emerged to streamline the payment process between merchants and customers' banks. The introduction of the Automated Clearing House (ACH) system in the 1970s further revolutionized payments by enabling electronic fund transfers between banks, improving speed and security.

The 1990s witnessed the emergence of online payment systems like PayPal, Amazon Pay, and Google Wallet. These systems offered consumers the convenience of making payments online without relying solely on credit cards. However, limitations persisted, such as restricted acceptance and security concerns.

In digital transactions, especially those conducted through electronic

(1) Regulation of e-payments in the UAE as businesses cash-in on cash-less solutions. Retrieved from The Legal 500: https://www.inhouselawyer.co.uk/legal-briefing/regulation-of-e-payments-in-the-uae-as-businesses-cash-in-on-cash-less-solutions/. 2017.

payment systems, additional parties may be involved beyond the traditional roles of drawer, drawee, and beneficiary. Some of the key parties in digital transactions include [1]:1-Payor: The individual or entity initiating the payment, often referred to as the «sender» or «payer.» They authorize the transfer of funds from their account to the payee.2-Payee: The individual or entity receiving the payment, often referred to as the «recipient» or «merchant.» They are the intended beneficiary of the funds transferred.3-Payment Service Provider (PSP): An intermediary that facilitates the electronic payment transaction between the payor and payee. PSPs offer payment processing, security, and other related services. Examples include PayPal, Stripe, and Square.4-Acquirer: The financial institution or bank that acts as an intermediary between the merchant and the payment network. They enable the acceptance and processing of payments made by customers through credit cards or other payment methods.5-Issuing Bank: The bank or financial institution that issued the payment instrument (such as a credit card or debit card) to the payor. The issuing bank authorizes and processes the payment on behalf of the payor.6-Card Network: In cases where card payments are involved, card networks (e.g., Visa, Mastercard, American Express) provide the infrastructure and protocols that facilitate the authorization, clearing, and settlement of card transactions.7-Clearinghouse: A financial institution or organization that facilitates the exchange, verification, and settlement of funds between the payor's and payee's banks. They ensure the smooth movement of funds between different financial institutions.8-Mobile Wallet Provider: In mobile payment transactions, a mobile wallet provider (e.g., Apple Pay, Google Pay, Samsung Pay) acts as a digital container for storing payment information and facilitating transactions using a mobile device.9-Trusted Third-Party: In certain digital transactions, trusted third-party services, such

(1) BIS Committee on Payment and settelment Systems. A glossary of terms used in payments and settlement systems. Retrieved from https://www.bis.org/cpmi/glossary_030301.pdf. 2003.

as escrow services or digital notaries, may be involved to provide additional security, verification, or dispute resolution services.

Therefore, new stakeholders emerged. Payment facilitators bridged the gap between merchants and payment processors, providing integration, fraud prevention, and chargeback management services. Aggregators acted as intermediaries, granting merchants access to various payment methods and providers. That is why specific parties are involved in a digital transaction may vary depending on the payment method, platform, and the nature of the transaction itself. Additionally, emerging technologies like blockchain may introduce new parties or roles, such as validators or miners, into the transaction process.

The European Union introduced the Payment Service Directive (PSD) in 2007 to regulate payment services, prioritizing safety and security in electronic payments. The PSD set guidelines for licensing payment institutions and established rules for processing and settlement. Facilitators, aggregators, and merchants play crucial roles in the payment ecosystem. Facilitators streamline payment processes, while aggregators offer unified platforms for processing payments. Merchants, as sellers of goods and services, accept payments from consumers [(1)].

In the Egyptian market, examples of aggregators and facilitators include Fawry, Paymob, Bee, Masary, and ValU. Fawry acts as a payment aggregator, offering diverse payment services through multiple channels. Paymob enables merchants to accept electronic payments via mobile point-of-sale solutions. Bee provides a mobile payment app for money transfers and purchases. Masary serves as an aggregator and facilitator, offering payment services and bill payments. ValU specializes in installment payment plans for online

(1) Official Journal of the European Union. DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366. 2015.

purchases. The extension of payment parties presents crucial questions from a legal standpoint. It is necessary to clearly allocate risk and obligations in complex legal agreements in order to avoid disputes. Strong legislative frameworks are essential for fraud prevention and consumer protection. Additionally, to maintain fair competition and protect consumers from anti-competitive practices, regulatory organizations like the CBE and FRA may need to step in.

As the digital banking landscape evolves, understanding the roles and responsibilities of various stakeholders becomes essential for maintaining a secure and efficient payment ecosystem. he expansion of digital banking methods and stakeholders in the payment landscape has significant legal implications. The following are some additional legal details to be considered[(1)]:

1. Regulatory Compliance: With the introduction of new payment methods and stakeholders, regulatory bodies play a crucial role in ensuring compliance with financial regulations. For instance, in the European Union, the Payment Service Directive 2 (PSD2) came into effect in 2018, further regulating payment services and strengthening security requirements. Compliance with these regulations is necessary to protect consumers and prevent fraudulent activities.

2. Data Protection and Privacy: The increasing use of digital banking methods involves the collection, storage, and processing of personal and financial data. Therefore, data protection and privacy laws, such as the EU's General Data Protection Regulation (GDPR), are relevant. Stakeholders must comply with these laws by implementing appropriate data security measures, obtaining consent for data processing, and ensuring transparency in handling customer information.

(1) EBA European Banking Authoroity. Guidelines on authorisation and registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

3. Risk Allocation and Liability: As the number of stakeholders in digital banking increases, it becomes essential to clearly define the allocation of risk and liability among the parties involved. This includes addressing issues such as unauthorized transactions, fraud, or disputes. Contracts and agreements between stakeholders should specify the responsibilities, liabilities, and dispute resolution mechanisms to mitigate legal risks and avoid potential conflicts.

4. Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF): The digital banking landscape must comply with AML and CTF regulations to prevent illicit activities. Financial institutions and payment service providers are required to implement robust Know Your Customer (KYC) procedures, monitor transactions for suspicious activities, and report any suspicious transactions to the relevant authorities. Failure to comply with these regulations can lead to severe legal consequences.

5. Intellectual Property: In the digital banking space, stakeholders may develop innovative payment methods, platforms, or technologies that are subject to intellectual property rights. Patents, copyrights, trademarks, or trade secrets may protect these intellectual property assets. Proper legal protection and enforcement of intellectual property rights are crucial to foster innovation and prevent unauthorized use or infringement by competitors.

6. Consumer Protection: As digital payments become more prevalent, consumer protection measures are paramount. Legal frameworks must address issues such as unauthorized transactions, fraudulent practices, dispute resolution, and transparency in pricing and terms. Consumer protection laws and regulations aim to ensure fair and transparent practices, protect consumer rights, and provide mechanisms for resolving disputes between consumers and payment service providers.

7. Cross-Border Transactions: The global nature of digital banking methods introduces complexities related to cross-border transactions. International payment regulations

3.4 Differentiating UC, SLA, and OLA Agreements in the Financial Industry

In the financial sector, UC, SLA, and OLA agreements have diverse functions. The framework for further agreements is laid forth by the UC, the anticipated service level is specified by the SLA, and the internal agreements between service providers are described by the OLA. The importance of these agreements in creating explicit relationships and guaranteeing responsibility in financial transactions is highlighted by real-world examples from the Egyptian FinTech market [1].

In the financial sector, UC (underlying contract), SLA (service level agreement), and OLA (operational level agreement) agreements have different functions [2]. While SLA and OLA outline service level expectations and internal service provider agreements, respectively, UC acts as the fundamental agreement. UC for lender-borrower loan agreements, SLA for payment gateway services, and OLA for payment processing services are a few examples of real-world FinTech products from the Egyptian market. These agreements are essential for forming distinct bonds and guaranteeing responsibility in business dealings.

The requirement for clearly specified agreements between parties involved in financial transactions becomes increasingly important as digital transactions and technology usage grow. This study seeks to distinguish between UC,

(1) IEEE. Service Level Agreement with Differentiated Reliability Requirements : Efficiency of Application in Communication Networks and On-Board Systems. Retrieved from https://ieeexplore.ieee.org/abstract/document/9744377. 2022.

(2) Robert E. Raygan, P. The Ultimate Big Data Enterprise Initiative: Defining Functional Capabilities for an International Information System (IIS) for Orbital Space Data (OSD). Retrieved from https://amostech.com/TechnicalPapers/2017/SSA/Raygan.pdf. 2017.

SLA, and OLA agreements while offering information about the Egyptian FinTech business.

A legally enforceable contract known as an «underlying contract» (UC) establishes the terms and conditions of a business partnership between two parties. It serves as the foundation for other contracts, such as SLAs and OLAs. UC outlines the goods, services, terms of payment, and other pertinent information, outlining the parties' respective legal responsibilities. For example, a UC can be constructed between lenders and borrowers for loan conditions in the Egyptian FinTech market, covering loan quantities, payback terms, and interest rates. The subsequent SLA and OLA agreements between the lender and the borrower are then built upon the UC.

An SLA, or service level agreement, is a contract between two parties that specifies the expected caliber of services to be offered. It describes service quality, performance measures, and sanctions for service violations. SLAs make sure that each party is aware of their responsibilities and hold the service provider responsible for delivering the contracted level of service. An SLA that specifies uptime, response time, and issue resolution time can be created between a payment gateway provider and an e-commerce platform in the Egyptian FinTech sector. This agreement commits the provider to providing a consistent and dependable payment gateway service and holds the provider accountable for any service level violations.

A contract known as an OLA (operational level agreement) describes the internal relationships between service providers working for the same organization. In order to achieve the anticipated service level for end customers, it defines the internal service level agreements between teams or departments. An OLA, including response time, issue resolution, and escalation procedures, can be established between a payment gateway provider and a payment processor in the Egyptian FinTech industry. Through this agreement, the two

parties will work effectively together to deliver dependable and consistent payment processing services [1]. The following details could be particularly specified in a SLA and should normally be included there: A brief description of communications, including reporting, review frequency, and timetable; a description of the service, product, or technology; the validity period and/or SLA UC change control mechanism; e) service hours like 9:00 to 17:00; date exclusions like weekends, holidays, crucial business seasons, and after-hours coverage; h) service provider UC: supplier liability and obligations, such as security; f) scheduled and agreed service interruptions, including notice requirements and the number of interruptions per period; g) customer obligations, such as proper system use and adherence to the information security policy; I) impact and priority standards; k) the complaints procedure; l) service goals; o) contingency plans to be used in the event of service interruptions, such as natural disasters and calamities; n) high-level financial management data, such as charge codes; a glossary of terms; supporting and related services, products, and technology; and any deviations from the SLA's requirements. m) Upper and lower workload limits, such as the ability of the technology, service, or product to sustain the specified number of users, volume of work, and system throughput.

The roles of UC, SLA, and OLA agreements vary in the banking industry. The UC lays the foundation for additional agreements; the SLA specifies the expected service level; and the OLA details the internal agreements between service providers. Real-world examples from the Egyptian FinTech industry serve to emphasize the significance of these agreements in establishing explicit relationships and ensuring responsibility in financial transactions.

(1) gSLM. Improving EGI's Service Level Management – an initial view. Retrieved from https://documents.egi.eu/public/RetrieveFile?docid=894&version=5&filename=ImprovingEGIServiceManagement.pdf. 2012.

3.5 PSD2 and Open Banking: Implications, Challenges, and its adaption in Egypt's Payment

Due to the importance of striking a balance between data security and innovation and the necessity of regulatory compliance for a thriving financial sector, the adoption of PSD2 and Open Banking in Arab nations, and Egypt in particular, has a variety of implications, challenges, and opportunities for the payment services industry. A legal framework known as PSD2 (Payment Services Directive 2) was created to encourage innovation, competition, and security in the payment services sector. Its adoption in Egypt might result in a market that is more inventive and competitive, which would be good for consumers. However, possible issues must be addressed by politicians, regulators, and industry stakeholders.

The introduction of PSD2 and Open Banking has significant implications for the financial sector, presenting both opportunities and challenges. While careful management of data privacy and security risks is crucial, these frameworks enable the development of customer-tailored and efficient financial products and services. Compliance with relevant regulations is essential for financial institutions and regulators in Egypt.

here are both opportunities and challenges presented by the implementation of PSD2 and open banking for the financial sector. These frameworks make it possible to create efficient and individualized financial products and services for customers, even though careful management of data privacy and security threats is essential. For financial institutions and regulators in Egypt, adherence to pertinent legislation is crucial.

The PSD2 standard was presented in 2015 and went into effect in January 2018. To improve the security, safety, and consumer protection of electronic payments, additional regulations were created. Furthermore, PSD2 required banks to share consumer data with outside suppliers, opening the payment services sector to fintech firms.

The introduction of PSD2 and open banking in the financial sector presents both opportunities and challenges. Though careful monitoring of data privacy and security issues is necessary, these frameworks enable the creation of effective and personalized financial products and services for customers. Compliance with relevant laws is essential for Egyptian financial firms and regulators.

In January 2018, the PSD2 standard, which was first introduced in 2015, became operational. Additional restrictions were made in order to enhance the security, safety, and consumer protection of electronic payments. Additionally, PSD2 mandated that banks exchange customer data with third parties, allowing fintech companies access to the payment services market.

3.6 Significance of Digital Identity in Banking and eKYC Processes

Digital identification is crucial to electronic Know Your Customer (eKYC) processes in the banking industry and offers many benefits, including increased security, streamlined customer onboarding, and increased operational effectiveness. These advantages have wide-ranging effects on numerous facets of the financial sector. Let's examine the significance of digital identity in many situations: [1].

Enhanced Security: By using digital identification solutions, you can authenticate yourself and verify your identity with greater assurance, greatly lowering your risk of fraud, identity theft, and unauthorized access. Financial institutions can strengthen security measures and guarantee that only authorized individuals have access to financial services by integrating cutting-edge biometric authentication techniques like fingerprint or face recognition during eKYC procedures.

(1) IEEE. THE URGENCY OF ELECTRONIC KNOW YOUR CUSTOMER (E-KYC): HOW ELECTRONIC CUSTOMER IDENTIFICATION WORKS TO PREVENT MONEY LAUNDERING IN THE FINTECH INDUSTRY. doi:https://doi.org/10.14710/dilrev.7.1.2022.34-52. 2022.

client Onboarding Process Simplified: Digital identification solutions simplify the frequently time-consuming and laborious process of client onboarding. These technologies reduce the need for manual labor, copious documentation, and protracted verification timeframes by automating identity verification procedures. By utilizing the power of automated algorithms and artificial intelligence, banks can quickly and successfully confirm the identity of their customers.

Enhanced Operational Efficiency: Digital identity solutions improve operational effectiveness within financial organizations by automating identity verification procedures. This results in substantial cost savings and quicker customer transaction turnaround times. Banks may expedite their operations and give clients a better overall experience by deploying eKYC procedures that make use of cutting-edge technologies and advanced data analytics.

Increased Financial Inclusion: The ability of eKYC and digital identification systems to promote financial inclusion is one of their great advantages. These technologies assist close the gap and integrate previously underserved groups into the financial system by allowing people without conventional identification credentials to access banking services. To reach a larger customer base, banks can use other forms of identification like mobile-based digital IDs.

The Payment Services Directive 2 (PSD2)'s main objectives are to advance open banking, improve the security of electronic payments, and stimulate innovation in the financial services industry. Although remote identity verification and authentication are not specifically mentioned in the regulation, they are extremely important in its context. To provide secure and practical distant identity verification between clients and service providers, financial institutions and fintech firms can make use of digital identity verification, eKYC procedures, biometric authentication, and two-factor authentication.

These steps improve the overall security and usability of electronic payments while ensuring PSD2 compliance.

3.7 Regulating Digital Identity and Digital Payment: Bottom of Form

Egyptian laws do not currently provide specific regulations regarding the complex new electronic identity verification methods and solutions. The legal implications of digital identity on legal capacity and digital payment in banks can be regulated within the framework of the Egyptian Civil Protection Act considers some potential regulations [(1)]:

1. Legal Capacity: Digital identity raises questions about the legal capacity of individuals to enter into binding agreements and engage in digital payment transactions. To address this, the Egyptian Civil Protection Act can establish provisions that recognize and regulate the legal capacity of individuals in the digital realm. This may involve defining the requirements for establishing digital identities and specifying the legal consequences of digital transactions.

2. Authentication and Authorization: Digital identity verification is crucial for ensuring the authenticity and authorization of individuals engaging in digital payment transactions. The Egyptian Civil Protection Act can outline the standards and procedures for verifying digital identities, including the use of reliable authentication methods such as biometrics or secure credentials. It can also specify the legal consequences of unauthorized access or fraudulent use of digital identities.

3. Privacy and Data Protection: Digital identity involves the collection, storage, and processing of personal data. To safeguard individuals' privacy and protect their personal information, the Egyptian Civil Protection Act can incorporate provisions that regulate the handling

(1) FATF. Digital Identity. Retrieved from https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html. March 2020.

of digital identity data by banks and other relevant entities. This may include requirements for informed consent, data security measures, and limitations on data sharing or retention.

4. Liability and Consumer Protection: The Egyptian Civil Protection Act can establish liability frameworks to address issues related to digital identity and digital payment transactions. It can define the responsibilities and liabilities of banks, payment service providers, and individuals in cases of unauthorized transactions, data breaches, or fraudulent activities. Consumer protection measures can be implemented to ensure fair practices, dispute resolution mechanisms, and remedies for individuals affected by digital identity-related issues.
5. Electronic Signatures and Records: Digital identity is closely tied to the use of electronic signatures and records in digital payment transactions. The Egyptian Civil Protection Act can recognize and regulate the legal validity and enforceability of electronic signatures and records, ensuring that they have the same legal standing as their traditional counterparts.

Regulating digital identity within the Egyptian Civil Protection Act can provide a comprehensive legal framework to address the legal implications of digital identity on legal capacity and digital payment in banks. By defining rights, obligations, and safeguards, such regulations can foster trust, security, and confidence in digital transactions while protecting the rights and interests of individuals involved.

4. Current Digital Payment Regulation in Egypt

This research explores digital banking regulation and the embracement of digital banking and FinTech through the Egyptian banking law of 2020

4.1 The Egyptian Banking Law of 2020: Embracing Digital Banking and Fintech

The Egyptian Banking Law of 2020, which replaces the existing 2003 law, has regulations that enable digital banking and financial technology (fintech). It strives to promote innovation while ensuring the financial industry's safety and stability. The following are key terms and requirements established in the law [(1)]:

1. Outsourcing: The law defines outsourcing as the delegation of banking activities to third parties under an agreement. Banks must obtain prior approval from the Central Bank of Egypt (CBE) and ensure the outsourcing arrangement does not jeopardize their operations' safety and soundness.
2. Financial technology (fintech): Fintech is defined as the utilization of technology to deliver financial services and products to customers. The law encourages fintech development and establishes a regulatory sandbox for testing new fintech solutions.
3. Direct debit: Direct debit refers to the authorization given by a bank customer to a third party for regular payment collection from their account. The law regulates direct debit transactions, requiring explicit customer consent before processing such payments.
4. E-money: E-money is the electronically stored monetary value issued against received funds for making payment transactions. The law regulates e-money issuers and mandates them to obtain a license from the CBE.

(1) L. S. Egypt's New Banking Law. Retrieved from https://www.lynxegypt.com/assets/pdfs/Business-Bulletin-Banking.pdf. November 2020.

5. Mobile payments: The law recognizes mobile payments as a valid payment method and provides regulations for mobile payment providers.
6. Digital onboarding: Banks can onboard customers digitally, using electronic identification and verification methods, subject to specific requirements.
7. Data protection: The law includes provisions on data protection and privacy, obligating banks and financial institutions to safeguard customer data and ensure confidentiality.

The Egyptian Banking Law of 2020 embraces digital advancements in banking and fintech, promoting a more innovative financial landscape while safeguarding customer interests and regulatory compliance.

In February 2019, the Central Bank of Egypt published Consumer Protection Instructions for Banks to lay the groundwork for the connection between banks and their customers at all stages of the transaction. Furthermore, the Central Bank of Egypt and the Banking Sector Law No. 194 for the year 2020 were both promulgated, with Articles 216 to 220 outlining the Central Bank's responsibilities for consumer protection. Furthermore, the Consumer Protection Sector was established with the primary goal of ensuring that consumer protection is a priority for licensed organizations. This is in addition to boosting consumer trust in the banking sector, safeguarding consumers' capacity to realize their rightful rights, and assisting them in making informed and competent financial decisions when interacting with licensed businesses[(1)].

4.2 Digital Banking Regulations in the Egyptian Banking Law 194 of 2020

4.2 Digital Banking Regulations in the Egyptian Banking Law 194 of 2020

The Egyptian Banking Law 194 of 2020 creates a regulatory framework for

(1) CBE. Consumer Protection. Retrieved from CBE. 2022.

digital banking, ensuring effective risk management and the establishment of a safe and efficient digital banking environment. The Egyptian Banking Law 194 of 2020 illustrates the government's acknowledgment of the importance of digital banking and its commitment to regulating the sector in a way that protects both clients' and the banking industry's interests.

The following is a brief study of articles in Chapter 4 of the aforementioned Act: -

Article 4 of the statute defines banking activities broadly, embracing both traditional and modern services, including electronic banking.

Banks are authorised to provide digital banking services under Article 38, subject to gaining approval from the Central Bank of Egypt (CBE) and adhering to the article's specific conditions.

Article 40 mandates that banks put in place appropriate technical and administrative protections to maintain the confidentiality, integrity, and availability of electronic banking data and transactions.

Article 41 authorises banks to outsource certain digital banking services with the CBE's consent and subject to specific criteria.

Article 42 allows banks to use financial technology (fintech) to provide banking services, subject to CBE approval and compliance with particular constraints. After getting a license from the CBE, banks are authorized to perform payment services utilising electronic payment instruments under Article 66. Furthermore, Article 200 of the Egyptian Banking Law 194 of 2020 defines direct debit as a payment service that allows creditors to collect funds from debtors' bank accounts using specified mandates.

Article 204 specifies the requirements for banks and other payment service providers to get CBE licences to conduct payment services.

Although Egyptian Banking Law 194 of 2020 does not categorise controls as preventative, directive, or detective, certain elements and desired outcomes can be understood as representing various sorts of controls.

Article 94, for example, mandates banks to have internal control systems and processes for managing operational risks, implying a preventative control strategy targeted at preventing or limiting operational hazards.

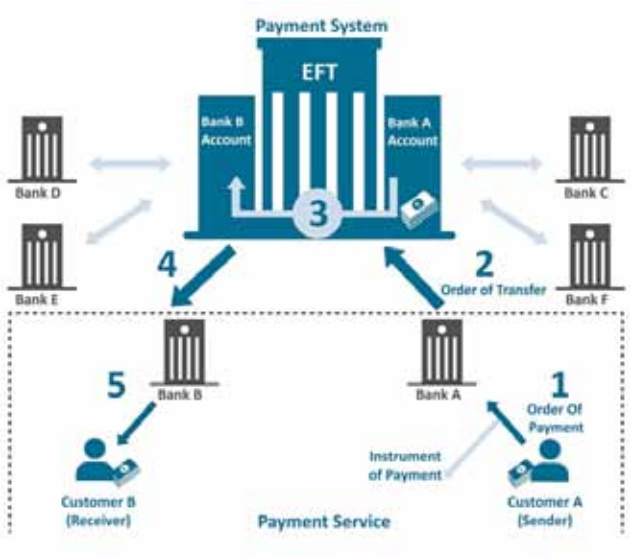
Article 50, on the other hand, requires banks to acquire CBE clearance before providing digital banking services, indicating a directive control directing banks to obtain CBE approval before providing such services. Furthermore, Article 52 requires banks to monitor digital banking transactions and report suspicious activity to the CBE, implying a detective control strategy focused on discovering and investigating suspected fraudulent or suspicious activity.

4.3 Understanding (PSOs) and (PSPs) in the Payment Industry

The working principle of the payment system involves the following steps: A customer who wants to send money provides a payment instruction to their bank, which is a participant in the payment system. The bank receives the payment instruction from the customer and submits it to the payment system as a «transfer order. «The money is electronically transferred from the sender bank's account to the receiver bank's account using the Electronic Funds Transfer (EFT) system. The receiver bank is notified of the transaction status.

The receiver bank receives information about the transaction and proceeds to pay the money to the intended recipient (payee) based on the information received from the payment system. Payment instruments used in this process can include personalized items like cards, mobile phones, and passwords, as agreed upon by the payment service provider and the user. Payment systems allow for seamless and fast interbank money transfers, enabling complex operations to be executed efficiently [1].

(1) CTMB, T. C. System, Payment Service and Payment. Retrieved from TCMB: https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/Payment+Service+and+Payment+System/#:~:text=In%20this%20case%2C%20the%20banks,used%20for%20interbank%20money%20transfers. 2023.



A multilateral system with participating institutions, including the system operator, is referred to as FMI (Financial Market Infrastructure). Payments, securities, derivatives, and other financial transactions are all cleared, settled, or recorded using FMIs. For participants, they provide standard operating procedures, technical infrastructure, and risk management frameworks. FMIs centralize financial transaction clearing, settlement, and recording, which boosts productivity, lowers costs, and lowers risks. Additionally, they support enhanced market transparency and efficient risk management. Some FMIs are important for maintaining financial stability and the monetary policies of central banks. Different organizational models, roles, and designs are possible for FMIs. They can take the shape of specialized banking organizations, groupings of financial institutions, or non-bank clearing entities [(1)].

Payment Service Operators (PSOs) are recognized organizations (we use the erm organization here and not companies' term as Central banks are sometimes operate payment systems especially the systematically most

(1) OICU, B. Principles for financial market InfraStructure. BIS Committee on Payment and Settelmemnt Systems. 2012.

important) that have received authorization from regulatory bodies like central banks to perform specific duties like clearing, netting, or settlement. These procedures, which form the foundation of the payment system, require special authorization and oversight.

However, a wider range of businesses that offer various payment-related services are included under the umbrella term «Payment Service Providers» (PSPs). Some examples of these services include payment processing, buying services, e-wallet services, payment gateways, and other payment facilitation activities.

PSPs may provide a variety of services; however, they do not have the necessary authorizations or licenses to handle clearing, netting, or settlement duties as this is the sole role of PSOs.

1. Clearing: Clearing is the process that takes place after a transaction to match and resolve payment instructions between the financial institutions of the payer and payee. It confirms the availability of the funds and verifies the accuracy of the transaction before proceeding to settlement.2. Netting: Netting simplifies complex financial transactions by merging numerous transactions between two parties into a single net amount. It offsets payment values, credits, or debts to determine the final payable or receivable amount. By reducing the number of individual transactions, netting promotes more efficient settlement.3. Settlement: The transfer of assets or money occurs during the settlement stage of a financial transaction. In order to fulfil the obligations outlined in the agreement, it includes the actual transfer of funds from the payer's account to the payee's account [(1)].

A merchant is a business or individual that sells goods or services and collects payments from customers. Merchants frequently manage their own

(1) BIS Committee on Payment and settelment Systems. A glossary of terms used in payments and settlement systems. Retrieved from https://www.bis.org/cpmi/glossary_030301.pdf. 2003.

payment processing and maintain open communication with customers. They can collect payments using a range of platforms, including ones that are physical, digital, or mobile [1].

An aggregator performs the function of a middleman by aggregating payment transactions from several merchants onto a single platform. It bridges the gap between the merchant and the payment service provider for smaller businesses or those without direct access to the payment infrastructure, expediting the payment process. Aggregators usually provide merchants with value-added services, including reporting, analytics, and fast onboarding [2].

By providing the necessary tools, resources, and services, a facilitator, also known as a payment facilitator or a payment service provider (PSP), enables businesses to accept payments. Facilitators often offer payment processing services that include transaction routing, payment gateway integration, and security measures. They might collaborate with a variety of shops and offer added services like risk management, fraud prevention, and customer support[3].

Therefore, PSPs focus on providing payment services to end users without directly participating in clearing, netting, or settlement in payment systems, whereas PSOs are largely in charge of these tasks. The distinct roles that PSOs and PSPs play in clearing, netting, and settlement are the key points of distinction between PSOs and PSPs in the context of payment services. PSOs are organizations that can perform one or more of these responsibilities, but PSPs lack the capacity or power to do so. Clearing is the process of

(1) EBA European Banking Authoroity. Guidelines on authorisation and registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

(2) EBA European Banking Authoroity. Guidelines on authorisation and registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

(3) EBA European Banking Authoroity. Guidelines on authorisation and registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

sending, comparing, and confirming payment instructions between financial institutions involved in a transaction. To expedite settlement and reduce the number of real transfers, netting involves balancing the amounts owed by many parties. The final step in the payment process is settlement when funds are sent from the payer's account to the payee's account to complete the transaction (1). Central banks and payment system operators are key players in this process since they enable the smooth operation of payment systems. The clearing, netting, and settlement operations are under their purview. They establish the framework, rules, and procedures required for participants to exchange money safely and successfully [(2)].

Conclusions

1. PSD2's facilitation of open banking has proven to be a revolutionary regulatory framework in Europe, encouraging competition, innovation, and client empowerment in the banking industry.
2. For Arab nations looking to enact open banking legislation, the ideas and directives described in PSD2 can be a useful guidance. To be in line with the judicial, regulatory, and economic realities of each Arab nation, these principles should be modified.
3. The success of open banking in fostering competition, innovation, and client empowerment is shown by the European experience with PSD2. It draws attention to the advantages that come from having regulations that permit safe data sharing and promote cooperation between banks and fintech businesses.

(1) CTMB, T. C. System, Payment Service and Payment. Retrieved from TCMB: https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/Payment+Service+and+Payment+System/#:~:text=In%20this%20case%2C%20the%20banks,used%20for%20interbank%20money%20transfers. 2023.

(2) BIS Committee on Payment and settelment Systems. A glossary of terms used in payments and settlement systems. Retrieved from https://www.bis.org/cpmi/glossary_030301. 2003.

Results

1. PSD2's support for open banking has established itself as a ground-breaking regulatory framework in Europe, promoting competition, innovation, and client empowerment in the banking sector.
2. The concepts and guidelines outlined in PSD2 can be a good guide for Arab countries wanting to pass open banking legislation. These principles should be changed to reflect the economic, judicial, and regulatory realities of each Arab country.
3. The European PSD2 experience demonstrates the effectiveness of open banking in promoting competition, innovation, and client empowerment. The benefits of having laws that allow for secure data sharing and encourage collaboration between banks and fintech companies are highlighted.
4. Greater Access to Financial Services: The PSD2 has aided in the creation of new and cutting-edge financial services, increasing their usability for a wider spectrum of customers. Customers can simply link their bank accounts to third-party applications through open banking, giving them access to customized financial products and services that are catered to their unique needs.
5. Development of the Fintech Ecosystem: PSD2 has encouraged the development of the European fintech ecosystem. Fintech businesses have attracted investments, and it has promoted cooperation between conventional banks and fintech firms. Innovative solutions, including peer-to-peer lending platforms, personal money management tools, and mobile payment apps, have emerged as a result of this collaboration.
6. Data-driven insights: PSD2's Open Banking has made it possible to securely share consumer data with their express consent.

7. Improved Financial Inclusion: Open banking has the potential to address the issue of financial exclusion by providing more inclusive financial services. Through open APIs and data sharing, fintech companies can develop tailored solutions for underserved populations, such as individuals with limited access to traditional banking services or those with thin credit histories.
8. PSD2 has encouraged digital transformation and service innovation in traditional banks. Traditional banks have been encouraged to embrace digital transformation and service innovation through PSD2. Fintech companies are teaming with banks to produce improved client experiences and launch new digital solutions by utilizing their knowledge and technology. This cooperation has increased the competitiveness of conventional banks and modernized legacy systems.
9. Reinforced Consumer Protection: PSD2 has provisions for robust customer authentication and improved security procedures to safeguard customers' financial information. Additionally, it specifies precise liability guidelines and dispute settlement procedures. These activities improve consumer protection, foster mutual respect, and advance a safe setting for financial transactions.
10. Opportunities for cross-border collaboration and growth have been made possible by the standardized framework established by PSD2. Fintech businesses in Europe can offer their services.

Recommendations

1. Policy makers should strive to establish an enabling regulatory environment that fosters innovation, protects consumer rights, and facilitates the rapid expansion of digital payment systems across Arab countries. This proactive approach will play a pivotal role in advancing the overall growth and development of the financial sector, promoting

greater financial inclusion, and driving the region's economic advancement in the digital age.

2. Establish Complete Regulatory Frameworks: Arab nations should create complete regulatory frameworks for open banking that cover information exchange, security standards, client protection, and interoperability requirements. These frameworks ought to strike a compromise between encouraging innovation and guaranteeing the security and confidence of customers.
3. Create Regulatory Sandboxes: By setting up regulatory sandboxes, open financial services may be tested and improved in a regulated environment. Before full-scale implementation, sandboxes enable collaboration among banks, fintech firms, and regulators to identify possible hazards and create adequate safeguards.
4. Promote cooperation and partnerships: Promote cooperation and alliances between conventional banks and fintech firms. This cooperation may encourage knowledge sharing, the creation of novel solutions, and the adoption of best practices.
5. Strengthen data protection and privacy rules: To guarantee the safe and responsible use of consumer data, strengthen data protection and privacy rules. To preserve consumer privacy and foster trust, implement reliable data encryption, consent management, and transparency measures.
6. Invest in technology and infrastructure: Establish the framework required for smooth integration between banks and FinTech, such as open APIs and secure data-sharing methods.

Bibliography

1. Hornuf, C. H. The emergence of the global fintech market: economic and technological determinants. Retrieved from https://www.researchgate.

net/publication/324050315_The_emergence_of_the_global_fintech_market_economic_and_technological_determinants. 2018.

2. World Bank. The World Bank. Retrieved from Payment Systems: https://www.worldbank.org/en/topic/paymentsystemsremittances#:~:text=Payment%20%26%20settlement%20systems%20are%20mechanisms,and%20help%20expand%20financial%20inclusion. 2022.

3. Thomsett, L. W. The Digital Banking Revolution. Deutche Nationalbibliografie. Retrieved from https://books.google.com.eg/books?hl=en&lr=&id=YDrEDwAAQBAJ&oi=fnd&pg=PR7&dq=The+financial+landscape+has+undergone+significant+transformations+throughout+history,+with+each+era+of+Fintech+bringing+unique+advancements+and+challenges.+Fintech+firms+have+had. 2019.

4. Welcome Sibanda, E. N.. Digital technology disruption on bank business models. International Journal of Business performance Managment. Retrieved from https://www.inderscienceonline.com/doi/abs/10.1504/IJBPM.2020.106121. March 30, 2020.

5. Impact of PSD2 on The Payment Services Market. Retrieved from sciendo: https://sciendo.com/article/10.2478/wrlae-2021-0008. October 26, 2021.

6. Dize Dinckol, P. O.. egulatory standards and consequences for industry architecture: The case of UK Open Banking. ELSEVIER. 2023.

7. Omarini, A.. Unbundling and re-bundling in the open industry of banking. Routledge. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9780429292903-15/fintechs-anna-omarini. 2021.

8. Resano. 2021.

9. Markos Zachariadis, P. O.. The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199. 2017.

10. Thomsett, L. W.. The Digital Banking Revolution. Deutche Nationalbibliografie. Retrieved from https://books.google.com.eg/books?hl=en&lr=&id=YDrEDwAAQBAJ&oi=fnd&pg=PR7&dq=The+financial+landscape+has+undergone+significant+transformations+throughout+history,+with+each+era+of+Fintech+bringing+unique+advancements+and+challenges.+Fintech+firms+have+had. 2019.

11. Thomas Walker. 2023.

12. Dize Dinckol, P. O. egulatory standards and consequences for industry architecture: The case of UK Open Banking. ELSEVIER. 2023.

13. API agreements: Why they matter & how to get them right. Retrieved from michalsons: https://www.michalsons.com/blog/api-agreements-why-they-matter-how-to-get-them-right/65117. April 12, 2023.

14. Michon, M. Understanding an API provider's privacy policy. Retrieved from Bearer : https://www.bearer.com/blog/understanding-an-api-providers-privacy-policy. April 22, 2023.

15. Simpson, J. How to Set SLAs for Cloud APIs. Retrieved from NORDIC: https://nordicapis.com/how-to-set-slas-for-cloud-apis/. September 27, 2022.

16. Theresa M. Weisenberger. Application Programming Interfaces (APIs). LexixNexis/ Practical Guidance , 3 4. 2022.

17. Exit Planning for Microsoft Cloud Services. Retrieved from microsoft.com: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWBkvx. August, 2020.

18. Innovation through BaaS and embedded finance. Retrieved from Finntech Futures: https://www.fintechfutures.com/2023/05/innovation-through-baas-and-embedded-finance/. 2023.

19. World Bank. Fintech and Financial Services: Delivering for development. Retrieved from World Bank Blogs: https://blogs.worldbank.org/voices/fintech-and-financial-services-delivering-development. February 24, 2023.

20. FinnTech Magazine. How BaaS unlocks vast opportunities for the banking sector. Retrieved from FinnTech Magazine: https://fintechmagazine.com/articles/how-baas-unlocks-vast-opportunities-for-the-banking-sector. February 12, 2023.

21. Li, G. Fintech, Bank Risk-Taking, and Risk-Warning for Commercial Banks in the Era of Digital Technology. Retrieved from https://doi.org/10.3389/fpsyg.2022.934053. July 22, 2022.

22. Federal Reserve Bank Of ST.LOUIS. Consumer Protection in the Fintech Era. Retrieved from https://www.stlouisfed.org/en/on-the-economy/2021/march/consumer-protection-fintech-era. March 28, 2021.

23. CTMB, T. C. System, Payment Service and Payment. Retrieved from TCMB: https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/Payment+Service+and+Payment+System/#:~:text=In%20this%20case%2C%20the%20banks,used%20for%20interbank%20money%20transfers. 2023.

24. SAMA issues draft regulation of payments law for public consultation. Retrieved from Argaam: https://www.argaam.com/en/article/articledetail/id/1550402. April 7, 2022.

25. SAMA issues draft regulation of payments law for public consultation. Retrieved from Argaam: https://www.argaam.com/en/article/articledetail/id/1550402. April 7, 2022.

26. Regulation of e-payments in the UAE as businesses cash-in on cash-less solutions. Retrieved from The Legal 500: https://www.inhouselawyer.co.uk/legal-briefing/regulation-of-e-payments-in-the-uae-as-businesses-cash-in-on-cash-less-solutions/. 2017.

27. BIS Committee on Payment and settelment Systems. A glossary of terms used in payments and settlement systems. Retrieved from https://www.bis.org/cpmi/glossary_030301.pdf. 2003.

28. Official Journal of the European Union. DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366. 2015.

29. EBA European Banking Authoroity. Guidelines on authorisation and registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

30. IEEE. Service Level Agreement with Differentiated Reliability Requirements : Efficiency of Application in Communication Networks and On-Board Systems. Retrieved from https://ieeexplore.ieee.org/abstract/document/9744377. 2022.

31. Robert E. Raygan, P. The Ultimate Big Data Enterprise Initiative: Defining Functional Capabilities for an International Information System (IIS) for Orbital Space Data (OSD). Retrieved from https://amostech.com/TechnicalPapers/2017/SSA/Raygan.pdf. 2017.

32. gSLM. Improving EGI's Service Level Management – an initial view. Retrieved from https://documents.egi.eu/public/ veFile?docid=894&version=5&filename=ImprovingEGIServiceManagement.pdf. 2012.

33. IEEE. THE URGENCY OF ELECTRONIC KNOW YOUR CUSTOMER (E-KYC): HOW ELECTRONIC CUSTOMER IDENTIFICATION WORKS TO PREVENT MONEY LAUNDERING IN THE FINTECH INDUSTRY. doi:https://doi.org/10.14710/dilrev.7.1.2022.34-52. 2022.

34. FATF. Digital Identity. Retrieved from https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html. March 2020.

35. L. S. Egypt's New Banking Law. Retrieved from https://www.lynxegypt.com/assets/pdfs/Business-Bulletin-Banking.pdf. November 2020.

36. CBE. Consumer Protection. Retrieved from CBE. 2022.

37. CTMB, T. C. System, Payment Service and Payment. Retrieved from TCMB: https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/Payment+Service+and+Payment+System/#:~:text=In%20this%20case%2C%20the%20banks,used%20for%20interbank%20money%20transfers. 2023.

38. OICU, B. Principles for financial market InfraStructure. BIS Committee on Payment and Settelmemnt Systems. 2012.

39. BIS Committee on Payment and settelment Systems. A glossary of terms used in payments and settlement systems. Retrieved from https://www.bis.org/cpmi/glossary_030301.pdf. 2003.

40. EBA European Banking Authoroity. Guidelines on authorisation and

registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

41. EBA European Banking Authoroity. Guidelines on authorisation and registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

42. EBA European Banking Authoroity. Guidelines on authorisation and registration under PSD2. Retrieved from EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2. 2022.

43. CTMB, T. C. System, Payment Service and Payment. Retrieved from TCMB: https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Core+Functions/Payment+Systems/Key+Issues/Payment+Service+and+Payment+System/#:~:text=In%20this%20case%2C%20the%20banks,used%20for%20interbank%20money%20transfers. 2023.

44. BIS Committee on Payment and settelment Systems. A glossary of terms used in payments and settlement systems. Retrieved from https://www.bis.org/cpmi/glossary_030301. 2003.