MED MSMEs
Policies for inclusive growth
THIS PROGRAMME IS FUNDED BY THE EUROPEAN UNION

Support to an Enabling Business Environment for MSMEs Development & Financial Inclusion

Facilitating MSME Access to Finance Through Fintech - The Case of the EU PSD2

April 2022

Contract number: 2018/401248

GOPA
WORLDWIDE CONSULTANTS

Contents

Acknowledgments

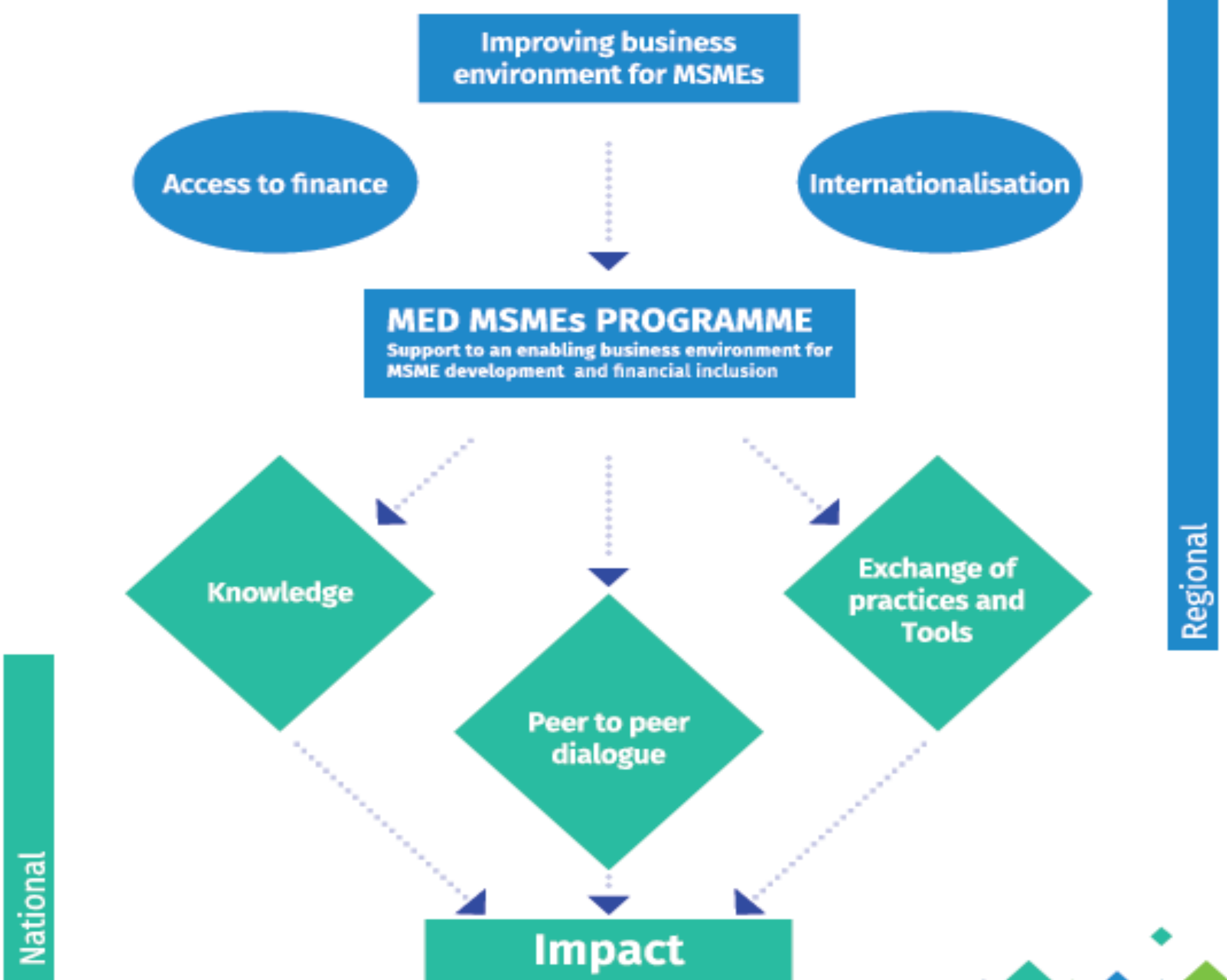
This discussion paper is the fruit of a collaborative process that gathered an extensive group of stakeholders, who we would like to thank, as they contributed to selecting the theme of “Facilitating MSME Access to Finance Through Fintech”, to the mapping of practices throughout the South Med region, the identification of challenges and opportunities, and the elaboration of recommendations.

They include SBACs, Banks, and government ministries and agencies as well as private sector representatives. We would like also to express our gratitude to the microfinance professionals who took part to the survey.

MED MSMEs
Policies for inclusive growth
THIS PROGRAMME IS FUNDED BY THE EUROPEAN UNION

FROM POLICES TO IMPACT

EU NEIGHBOURS south



The **MED MSMEs Programme** (2018-2023) is funded by the European Union. It aims to convene stakeholders and support dialogue at regional level to inspire policies and regulatory reforms for Micro, Small and Medium Enterprises (MSMEs), in particular on the internationalization and access to finance dimensions.

The Programme in a nutshell

In line with the elaboration of policies for inclusive growth in the EU Southern Neighbourhood, the European Union-funded MED MSMEs Programme builds on a national participatory approach, international best practices and regional initiatives to foster the formulation and implementation of integrated policies and instruments supporting the development of MSMEs.

What we do ?

The EU-funded MED MSMEs programme is seeking to place MSMEs at the centre of sustainable growth in Europe's Southern Neighbourhood region.

The Programme contributes to improve the MSMEs business environment thanks to knowledge-based South-South and South-North dialogue and the elaboration of policy responses that are more adapted to the needs of MSMEs and their support ecosystems.

The MED MSMEs Programme is implemented with partner countries, namely Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine*, Syria** and Tunisia, in close collaboration with the network of national Small Business Act (SBA) Coordinators who are country focal points. The SBA Coordinators and members of the working groups form a community of practice which constitutes a regional platform supported by the Programme.

How we do it ?

The selection of activities and their implementation is driven by a set of 5 principles:

- Mobilize the expertise and disseminate the know-how required to elaborate policies that translate into impact ("From policies to impact").
- Prioritize activities that can leverage the benefit of a regional approach to enhance impact at national level by capitalizing on existing initiatives and programmes.
- Combine top-down and bottom-up approaches by capitalizing on national working groups.
- Articulate cross-cutting and vertical dimensions in close coordination with other regional and bilateral programmes.
- M**ainstream gender into all activities.**

Executive Summary

This report summarises the findings and recommendations of the assignment entitled "Awareness Raising of EU PSD2 as a Catalyst for FinTech and MSME Access to Finance" which assessed how, in the European Union, the adoption of the Payment Services Directive 2 (PSD2) exerts a positive impact on MSME access to finance, by allowing and stimulating the development of fintech services based on strengthened payment security, data protection and sharing.

Regarding methodology, this report seeks to answer several key questions about Europe´s experience and how these experiences could apply to the Southern Mediterranean.

- What were the concerns and risks about PSD2 and how were they overcome?
- What other legal, regulatory, or technical structures were needed as prerequisites to PSD2?
- What was the process that led to PSD2?
- How and why was PSD2 implemented?
- What can we observe at this early stage of PSD2´s impact?
- What are the gaps between where Europe was when it began PSD2 implementation and where Southern Mediterranean countries are now? What changes would be made to overcome these gaps and prepare for potential PSD2 implementation?
- Why and how would the Southern Mediterranean want to implement PSD2-style rules?

Chapter 1 of this paper discusses the global changes sweeping through the financial sector due to digitalization and goes on to discuss the goals of MED MSME Programme to support dialogue and engagement around these changes. The financial sector worldwide is undergoing a profound transformation driven by digitalization, the use of big data, artificial intelligence and the emergence of new entrants providing unheard-of solutions that are impacting the daily life of individuals and corporates. PSD2 is a key structure in bringing these changes in Europe, especially as a prerequisite to Open Banking. These new solutions are expected to bring customised financial products and services to MSMEs and consumers who may either have been un-bankable under traditional scoring models, or who could not find financial services that met their needs. The global transformation of the financial system is the fruit not only new technology, but also of a long series of regulatory changes. In Europe,

the regulatory challenge was taken up by the adoption 15 years ago of the Payment Services Directive that created a single market for payments by providing the legal foundation for a Single Euro Payments Area. In 2013, a version 2 of the directive was adopted to facilitate the integration of new entrants, allow for EU/Rest-of-the-World transactions, further secure payments of the Directive took until 2020, reflecting an unprecedented effort of harmonisation with far reaching impact. This process is discussed in more detail in chapter 5.

Chapter 2 discusses the basics of what PSD2 is and its role as a pre-requisite for Open Banking. At its most basic, PSD2 created the common standards through which banks could share data, through which non-banks could access this data, through which customers could "opt-in" to be part of this data sharing and through which appropriate cybersecurity standards could be established. There were other rules also foundational for Open Banking as well, most notably including GDPR contributing to the foundation for this through rules governing protection of consumer data, and PSD1 allowed for cross-border payments with one common European market. These rules governing data protection and cross-border payments were necessary pre-cursors to PSD2 to be able to be implemented, and for the growth of Open Banking in Europe.

Chapter 3 presents the global trend towards Open Banking is appearing in every region, from North and South America to Sub-Saharan Africa to the Gulf to South, Southeast and East Asia, and then looks at how a PSD2-style rule could lead to Open Banking in the Southern Mediterranean. Taking the train of digital finance by capitalizing on the creation of local big data – Open Banking – is the next key to competitiveness, and as other regions are already moving into this space, Southern Mediterranean policymakers must be aware of the pros and cons of doing so, and to ensure they are not left behind.

Chapter 4 focuses on client data protection, and especially what data protection rules are already in place in the Southern Mediterranean. A major challenge for PSD2´s implementation was to ensure that personal data remains protected, following the standards of the General Data Protection Regulation (GDPR). New actors can access this data under such a system, but they must ensure they have the capability to follow data protection rules, including the cybersecurity strength to protect their systems.

Chapter 5 details how PSD2 was implemented in Europe, summarizing the institutional reform process of implementing PSD2 in Europe, as well as a description of Europe´s experience with PSD2. Key to this experience is that it was a gradual implementation, over many years, with dialogue and inclusion of relevant stakeholders. This chapter also discusses methods Europe has used to monitor the impact of PSD2 and potential needs for changes in its implementation. For example, in October 2021 a call for services was made to analyse potential challenges and flaws in PSD2 implementation as well as making recommended changes.

Chapter 6 looks finally at how PSD2 could be implemented in the Southern Mediterranean as well as making specific recommendations of next steps for the Southern Mediterranean. These steps start with information dissemination and dialogue, and if all parties agree that a PSD2-style rule is the necessary next step, country and regional level working groups can work to develop the necessary rules for implementation.

Chapter 7 delivers conclusions and recommendations. The paper concludes that PSD2-style rules can be a catalyst for economic growth, offering increased access to finance for MSMEs while also giving birth to new sectors of FinTech and thus also new MSMEs and startups. While countries globally are moving to create PSD2-style rules for the economic growth opportunities it can bring, not moving in this space risks falling behind as non-regional financial service providers develop new products and services for their own markets, and eventually will bring those offerings to the Southern Mediterranean.

Moving forwarded, it is recommended to create national working groups who would evaluate the current financial sector policies and regulations, identify needs to develop the current financial system, strategize the implementation plan, and find resources for implementation. These national working groups should include both public and private sectors such as banks, FinTech companies, consumers and MSMEs. These working groups can build on this paper to discuss further the roles of specific government agencies as well as self-regulatory organizations and requirements for standardization such as approaches to licensing, legal, consent and privacy, user experiences and operations specifications (standardization of APIs, cybersecurity rules and the establishment of regulatory sandboxes). Regulators should then move forward in gradually establishing rules, giving sufficient time for implementation, while at the same time being the force that pushes forward the financial services sector to offer new innovations.

Appendices at the end of this paper discuss individual country analyses, a list of acronyms used in this paper, and finally a series of case studies related to Open Banking about the European Union and specific countries in the European Union, the United Kingdom, the United States and China.

Next steps: This working paper will be presented at a webinar and disseminated for feedback. National and regional working groups should be formed, and the MED MSMEs Programme should be made available to provide guidance to working groups, both in organizing the events as well as in drafting specific national action plans based on the discussions of these working groups.

1. Opening new horizons

1.1 A revolution in the making

The financial sector worldwide is undergoing a profound transformation driven by digitalization, the use of big data, artificial intelligence and the emergence of new entrants providing unheard-of solutions that are impacting the daily life of individuals and corporates.

As always in the financial sphere, this ***revolution has been the fruit of a long regulatory reform process***, a process that was delicate as it required - altogether - to integrate innovation while maintaining the stability of the financial sector, protecting individuals with regards to the processing of personal data while allowing free movement of such data, and enlarging the scope of the traditional financial sector to information-based companies that are not precisely financial institutions.

MSMEs are among the core beneficiaries of the financial sector transformation as it allows new business models emerge and enhances commercial innovation leading to new products targeted towards MSMEs, as well as new opportunities for them to enter the marketplace with their own new products.

In Europe, the regulatory challenge was taken up by the ***adoption 15 years ago of the Payment Services Directive*** that created a single market for payments by providing the legal foundation for a Single Euro Payments Area. In 2013, a version 2 of the directive was adopted to facilitate the integration of new entrants, allow for EU/Rest-of-the-World transactions, further secure payments of the Directive took until 2020, reflecting an unprecedented effort of harmonisation with far reaching impact.

The MED MSMEs Programme focusing notably on disseminating practices on MSME alternative and innovative finance was tasked with the elaboration of a synthetic document that would contribute raising the awareness in the South Med region on the PSD principles and tools, on the processes that allowed the adoption of such a directive, and how it is expected to impact MSME-driven growth and job creation.

Hence, the present report summarises the ***findings and recommendations of the assignment entitled "Awareness Raising of EU PSD2 as a Catalyst for FinTech and MSME Access to Finance"*** that was meant at assessing how, in the EU, the adoption of the Payment Services Directive exerts a positive impact on MSME access to finance, by allowing and stimulating the development of fintech services based on strengthened payment security, data protection and sharing.

The purpose of raising awareness of PSD2 is multifaceted. As shown in the chart below, as banks begin to share data, a system patterned on PSD2 create rules on both how and what data is shared, as well as common security rules on how to protect the data to be shared.

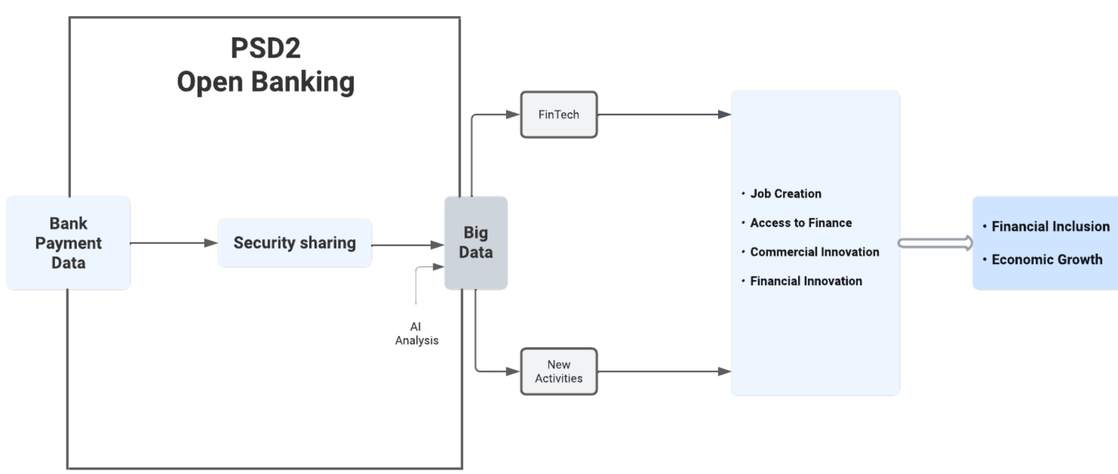
The big data that comes from this sharing can be analysed by Artificial Intelligence and can lead to not only new companies developing in the FinTech sector, but also traditional financial institutions using this expanded data set to develop new activities creating value and attracting investment.

Beyond European countries adopting PSD2, Australia, Norway, and Iceland are at the forefront with the likes of Thailand, Japan, Mexico, and Brazil following quickly behind, while Nigeria, and Uganda also have developed Open Banking regulations. This trend towards global banking is global wave, not only something from Europe.

In total, this growth in the FinTech sector and offering of new activities implemented by banks can lead to job creation, new access to finance and commercial and financial innovation

In total, this growth in the FinTech sector and offering of new activities implemented by banks can lead to job creation, new access to finance and commercial and financial innovation.

PSD2: enhancing financial inclusion and economic growth



Source: MEDMSME Research Team 2022

1.2 Supporting dialogue and engaging stakeholders

A regulatory reform process that can result in a more digitalized financial sector is complex, lengthy, and requires the adhesion of many traditional and less-traditional stakeholders.

It also raises ***legitimate concerns and trigger resistances to change*** –by regulators, customers, and service providers - that can be addressed by raising the level of information on the state of the art in the region and in Europe, discussing the pros and cons of the emerging solutions and assessing the state of play to sketch a roadmap allowing to materialize the positive externalities of the current transformation while mitigating possible negative impact.

Taking as an assumption that this transformation is comprehensive and inevitable and acknowledging that the ***tsunami of digital finance has already reached the shores of the EU Southern Neighbourhood***, the MED MSMEs Programme decided to contribute to inform the dialogue and engage the multitude of stakeholders involved.

Taking the train of digital finance by capitalizing on the creation of local big data is the next key to competitiveness

It will result in greater innovation, more exports, value creation, investment and jobs…

The specific objectives of the assignment, reported here, are that awareness is raised about the PSD2, the Open Banking and the Banking 4.0 revolutions in the Southern Mediterranean. Stakeholders will be engaged through webinars gathering the members of the access to finance working groups at both the national and regional levels.

2. Open banking and PSD2 as drivers of inclusive growth

2.1 Open banking underlying principals

To understand how the PSD2 was implemented, it is important to grasp its dynamics, the underlying principles, and the *modus operandi*.

At its most basic, ***Open Banking is the system by which non-banks and even non-financial institutions can have access to financial data that customers opt to share***, and as such technology companies, retailers, FinTechs, neobanks and non-bank financial institutions can use this data to offer new financial products, based on analysis of this data, which previously was only available to the banks, as demonstrated in the graphic below.

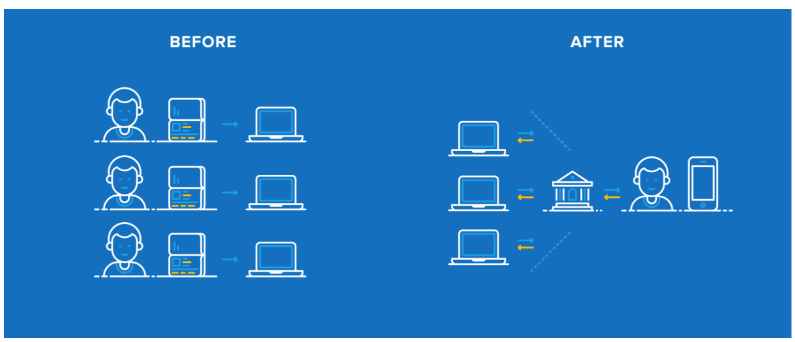
Open finance also provides lenders with a broader picture of customers' financial situations and increasingly involves the ***sharing of data by other service providers*** such as telecommunication companies (telcos). Data from smartphones and AI is also being used by non-banks to create economic identities for unbanked people through alternative scoring algorithms.

The ***proprietary nature of lending***, for example, means that credit granting relies more on the scope of data than any unified framework, thus standardized marketplaces offering competing loan products will benefit from consistency. Lenders will rely more for their lending decisions on consistent data gathered simultaneously from various sources. Examples of this include spending patterns, outstanding debt, and potential risks if the borrower, and these can be treated through an institution's own algorithms to provide a more informed underwriting to the benefit of the client.

Open banking is revolutionary with respect to underwriting which uses non-conventional credit sources and AI for its decision-making process. This digital change causes benefits to customers as these non-traditional data points, such as payment histories from a current account, allow banks to extend credit products in situations where they would not have following traditional lending models. Niche and narrow lenders were first to pioneer this alternative data gathering for underwriting starting 2016. This has worried the European Central Bank, which in its 2017 Fintech application guide[1] made it clear that where alternative data sources are used and that regulators will assess existence and support of adequate risk mitigation safeguards including capital. Open banking is allowing more non-bank financial institutions to enter the credit market, with the retailer Amazon as one of the first to use these types of underwriting approaches

An important set of tools for open banking are Advanced Programming Interfaces (APIs). APIs are software interfaces that allow data to be accessed from one computer network to another. This is what allows the systems of a bank to share data with other banks as well as non-bank financial service providers, sharing their data across networks. In a survey by the Economist Intelligence Unit in 2020, 87% of countries surveyed reported that they have some form of APIs in place, laying the foundation for further development.[2] Usage of these APIs also depends on the degree of customer confidence in sharing their data, interoperability, enhanced user experience, and the added value of products and services, which is done through API's. Leveraging open-source technology, API's foster the influx of open data to be shared, greater financial transparency, hence added value of products and services.

The integrative power of APIs



Source [*WAAR.CH*]

At its most simple, with PSD2 allows consumers and small businesses to directly interact with one public API, which will then help them find the best offers from various financial institutions, instead of separately having to interact with each financial institution.

An **overview of the interactions in an open banking system** can be seen below.
On the **customer side**, we see tailor-made products being developed based on big data collected from payment trends and the ability to have alternative credit scoring models. Transparency in the system, drawing together data from various points, also allows transparency in the system, where consumers and MSMEs can compare the levels of fees for various services.

---

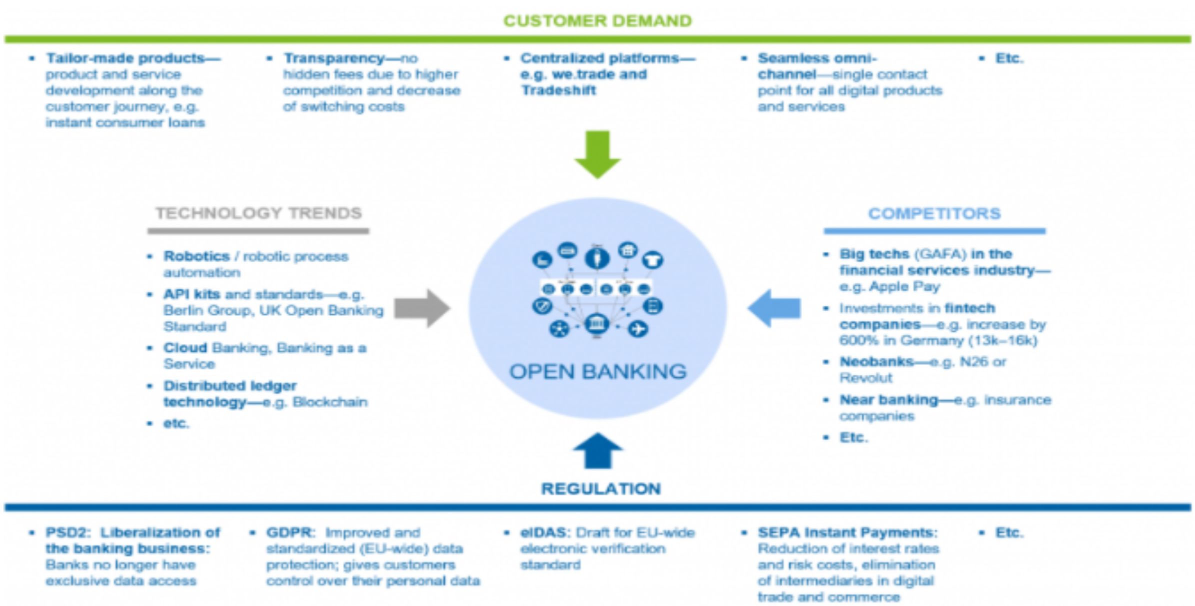
[1] Guide to assessments of fintech credit institution licence; https://www.bankingsupervision.europa.eu

[2] https://www.temenos.com/wp-content/uploads/2021/02/Temenos-Open-banking-VFinal-1.pdf

Centralized platforms pull this data together, giving one point through which non-bank financial institutions can also make analysis and develop new products and services.
The pool of competitors is wider, as "non-bank financial institutions" can also include organizations that are traditionally not thought of as financial service providers, such as Apple, Google or Amazon, as well as new FinTech companies, Neobanks and companies providing "near banking" services, such as insurance companies.

New technologies all also converge to be implemented in the open banking space, ranging from blockchain to cloud computing, and as shown as well in the chart below, a bevy of new regulations was needed to structure this system to work efficiently and securely.

An overview of the open banking ecosystem



Source: [BANKING HUB]

Open banking plays the role of an honest broker that contributes to disintermediation of traditional channels, to decreasing the costs of services and results in better-informed decision-making processes by customers, whether MSMEs or consumers. It is therefore a ***competition enhancer to the benefit of the demand side***.

2.2 Open banking and PSD2

Europe´s Payment Services Directive 2 (PSD2) is a ruling that sets the groundwork for Open Banking to take place. At its most basic, PSD2 created the common standards through which banks could share data, through which non-banks could access this data, through which customers could "opt-in" to be part of this data sharing and through which appropriate cybersecurity standards could be established. There were other rules also foundational for Open Banking as well, most notably including GDPR contributing to the foundation for this through rules governing protection of consumer data, and PSD1 allowed for cross-border payments with one common European market. These rules governing data protection and cross-border payments were necessary pre-cursors to PSD2 to be able to be implemented, and for the growth of Open Banking in Europe.

2.3 Are client data protection principals pertinent in PSD2?

The PSD2 has introduced several novelties in the payment services field. While it creates new opportunities for consumers and enhances transparency in such field, the application of the PSD2 raises certain questions and concerns in respect of the need that the data subjects remain in full control of their personal data. The General Data Protection Regulation (GDPR) applies to the processing of personal data including processing activities carried out in the context of payment services as defined by the PSD2. Thus, controllers acting in the field covered by the PSD2 must always ensure compliance with the requirements of the GDPR, including the principles of data protection set out in Article 5 of the GDPR, as well as the relevant provisions of the ePrivacy Directive. While the PSD2 and the Regulatory Technical Standards (RTS) for strong customer authentication and common and secure open standards of communication contain certain provisions relating to data protection and security, uncertainty has arisen about the interpretation of these provisions as well as the interplay between the general data protection framework and the PSD2.

On July 5 2018, the EDPB issued a letter regarding the PSD2, in which the EDPB provided clarifications on questions concerning the protection of personal data in relation to the PSD2, in particular on the processing of personal data of non-contracting parties (so called 'silent party data') by account information service providers (hereinafter "AISPs") and payment initiation service providers (PISPs), the procedures with regard to giving and withdrawing consent, the RTS and the cooperation between account servicing payment services providers (ASPSPs) in relation to security measures. Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges. These guidelines aim to provide further guidance on data protection aspects in the context of the PSD2[3].

2.4 Expected benefits

As a high level, it is expected that Open Banking will allow new financial products and services to be developed, to the benefits of not only consumers and businesses who have access to additional financial products, but also to banking and non-banking financial institutions who have new avenues to reach customers, increasing their customer base to include organizations or individuals who previously were unbanked as well as customers in markets outside of their domestic market. Overall, this competition within the financial services sector and availability of new products is expected to lead to greater economic growth.

In regard to what we have seen so far of this process, there already have been cases of banks benefiting through genuine partnerships with new FinTechs, through investing in and outright buying some of the most successful FinTechs and opening up API to the FinTech community, drawing more developers to work on new solutions and products.4 Through these kinds of partnerships, we are seeing banks able to maintain and grow their relationships while FinTechs work through existing banking relationships and even sometimes focus on back-end support for the banks instead of reaching out directly to customers.

[3] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

[4] Open banking: Is that it? | Frontier Economics (frontier-economics.com)

This saves the FinTechs from taking the time to build up trust with new consumers while at the same time allowing the banks to increase their operating efficiencies, and these kinds of partnership would not have been possible without PSD2.

We have also seen that since PSD2´s adoption there was a temporary surge in "PayTech" startups in Europe. As well, after national levels rules were implemented, there was a decline in new entrants to the market, but it remained higher than before the adoption of PSD2, indicating that there was a positive impact. Part of this growth is cited to have come from the larger markets, which were expected to cause growth in the sector, and regulatory sandboxes to support the development of the sector.[5]

2.5 How to monitor the legislative impact?

It is important to note that PSD2 is very specific in including a clause on how to monitor the impact of PSD2. Specifically, the review clause in Article 108 of PSD2 requires the Commission to report on the application and impact of the Directive to the Co-legislator (the European Parliament and the Council), the European Central Bank and the European Economic and Social Committee. The review clause in Article 108 of PSD2 even specifies the content of the Commission's report. To implement this, a call for services was issued in October 2021 to identify challenges and benefits that may have arisen because of PSD2 implementation and to identify areas where amendments may be appropriate.

PSD2 is Europe´s implementation of Open Banking and it can be expected to lead to greater access to credit and other financial products for MSMEs and consumers alike, sparking further economic growth. However, it remains early to see the full results of PSD2.

3. Open Banking Globally and in the Middle East and North Africa Region

3.1 Open banking globally

The global Open Banking market is anticipated to rise at a considerable rate during the forecast period, between 2021 and 2026. In 2020, the market grew at a steady rate and with the rising adoption of strategies by key players, the market is expected to rise over the projected horizon. The global open banking market grew from US$11.79 billion in 2020 to US$15.13 billion in 2021 at a compound annual growth rate (CAGR) of 28.4%. The change in growth trend is mainly due to the companies stabilizing their output after catering to the demand that grew exponentially during the COVID-19 pandemic in 2020. The market is expected to reach US$37.77 billion in 2025 at a CAGR of 25.7%[6].
Globally, 36 countries and the European Union are host to Open Banking initiatives and thus it is imperative that central banks of the Southern Mediterranean take inspiration from the European model, as well as other Open Banking models, to allow FinTechs to develop and create new and innovative financing solutions. Analysis of the number of licences obtained reveals that the top ten countries include all five largest EU member states in terms of population and GDP. The graphic below from Penser, issued in 2019, shows how widespread Open Banking already was by that year.

[5] The impact of Payment Services Directive 2 on the PayTech sector development in Europe - ScienceDirect
[6] Global Open Banking Global Market (2021 to 2030) – December 2021

Penser, 2019 Study.

This move towards PSD2-style Open Banking is part of a larger global change. Economic models around the world have been changing for more than 10 years. We are moving from a stock economy (products, data) to a flow economy where everything is interconnected and managed by artificial intelligence algorithms (UBER, Netflix, Airbnb, etc.). The economic fabric of companies in the Southern Mediterranean is still in stock mode and the catalyst for transformation can only come from financial partners because they can secure, store and trace any transaction. The role of banks is becoming crucial for the transformation of the economy. The creation of value through business ecosystems requires the opening of data and therefore Open-Banking. Companies need to work together in complete transparency, to aggregate accounts in real time with the financial system, to have immediate scoring for credit and above all secure payments.

If central banks do not act on their own, there is a risk that global and regional banks developed in other financial centres will increase their lead in innovation and even start to move into Southern Mediterranean markets. The "Uberization" of payment services and the PSD2 directive have begun to reshape the financial landscape on a European scale, offering new professions, new financial services, new positioning, new economic model, new experience.

New global competition to offer the best service to customers forces banks to find new ways to offer services with real added value for its customers, or to engage in a price war by offering account management services with the risks losing its position as a privileged interlocutor which today allows it to sell other banking services.

3.2 Open banking in the South MED region

The MENA region is gradually emerging as a new open banking microcosm, and it is revealing different priorities among its respective countries who previously operated according to distinctive regulation-driven approaches, depth, and speed. Within the region, the Southern Mediterranean countries, except for Israel, have not been as active in taking steps towards open banking as the Gulf Cooperation Council (GCC) member countries.

Open Banking has now arrived in the Middle East, with The Central Bank of Bahrain (CBB) launching the Bahrain Open Banking Framework in October 2020. Saudi Arabia also recently announced a draft regulation, which is expected to be implemented by mid-2022. Other Middle Eastern countries, such as the United Arab Emirates (UAE), Kuwait, Oman, and Egypt are likely to follow suit[7].
In a context where SMEs are diverting to alternative financial service providers for better products and services, PSD2 and open banking are likely to accelerate this division. Banks will need to do more than to deliver their existing products better, they will need to enhance their digital and data analytics capabilities and develop an ecosystem of partners to improve personalization and deliver more value-added services beyond simply meeting SMEs' financial needs. Implementation of a PSD2-style rule would give them access to the level of data needed to do this, as well as sparking the creation of new FinTechs who could be not only competitors but also partners to banks.

A sample of the region shows the degree to which many countries in the region are already moving towards and implementing the frameworks needed for Open Banking.

Policy enabling environment: Examples from selected MENA countries

	Data Protection Framework in different forms	Cybersecurity Framework in Place	Planned Open Banking Framework	Open Banking framework in Place
Egypt	✓		✓	
Jordan	✓	✓	✓	
Morocco	✓	✓	✓	
Bahrain	✓	✓		✓
UAE	✓	✓	✓	

Source: MEDMSME Internal Research

[7] https://treasury-management.com/blog/open-banking-in-the-middle-east-driving-adoption/

A key challenge in the MENA region as a whole is Know-your-customer (KYC) verification. This is one of the most important APIs for open banking innovation in the Arab region. In the MENA region the GCC is leading, but there is also an ***acceleration of the adoption of eKYC solutions*** occurring in cash-dependent countries, such as Jordan and Morocco, where remote onboarding onto e-wallets has been important during COVID-19 so people can receive government support.

As the biggest impact to be expected relies in retail banking, payments and consumer lending, where many banks and non-bank financial institutions (NBFIs) are considering alliances with other non-financial service providers or platforms, yet with some push-back:

- Most Institutions regard PSD2 model or Open Banking as an opportunity but remain wary of the threats it poses to their business models, and the investment needed.
- Customers' awareness regarding the use of digital banking channels reveals significant differences within the region, as they seem still captive to legacy models, be it cash, or physical interaction with FSP's.

4. Overview on client data protection principals in the South MED region[8]

EGYPT

Egypt recently introduced the Law on the Protection of Personal Data ('the Data Protection Law') issued under Resolution No. 151 of 2020. The Executive Regulations for the Data Protection Law have not been issued yet even though they should have been issued by the Minister of Communications and Information Technology within six months from the date on which the Data Protection Law entered into force in Egypt. It is worth noting that any entity that is subject to the Data Protection Law is required to legitimise its position with the provisions of the Data Protection Law within a year starting from the issuance date of its Executive Regulations.

The Data Protection Law reflects the European General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), as it aims to establish various standards and rules which safeguard the rights of individuals in Egypt regarding their personal data. Prior to the introduction of the Data Protection Law, data protection was only governed through various legislations in Egypt such as the Constitution of the Arab Republic of Egypt ('the Constitution'), the Penal Code No. 58 of 1937 ('the Penal Code;) and the Law No. 175 of 2018 on Anti-Cyber and Information Technology ('the Cybersecurity Law'). Therefore, the issuance of the Data Protection Law consolidates the rules and regulations regarding data protection and privacy in Egypt.

Data breach notification

According to Article 7 of the Data Protection Law, data controllers and data processors are required in cases where they become aware of any breach or violation of personal data to report such

[8] https://www.dataguidance.com

breach/violation to the DPC within 72 hours or immediately in cases where such breach or violation is related to national security. In all cases, both data controllers and data processors shall notify the data subject within three days as of the date on which the relevant breach was reported to the DPC

ISRAEL

Data Protection in Israel is governed primarily by the Protection of Privacy Law and enforced by the Privacy Protection Authority. The law covers collection and use of personal data and sensitive data, sets the rights and obligations of the parties collecting and using the data, including security requirements with respect thereto, and sets the rights afforded to individuals whose data is collected and used.

Data breach notification

In certain circumstances, a database owner may be required to conduct a data security risk assessment. Such risk assessment will be conducted at least once every 18 months. Database owner shall document any security incident, and in certain circumstances inform the PPA of such incident.
A database owner is responsible for documenting any incident that raises concerns as to the integrity of the data or any unauthorised use of the data. If a severe security event occurs, then the database owner shall inform the PPA immediately, and not later than 72 hours from its occurrence and shall report the steps that were taken following such an event. The PPA may order the database owner to inform the data subjects that may be affected by the security event.

Sectoral obligations

In addition to the general obligation to notify a security event, entities in certain sectors are subject to more specific legislation that imposes on them additional duties. Notably, the Supervisor of the Capital Market, Insurance and Savings Authority ('the Capital Market Supervisor') of the Ministry of Finance published a circular regarding cyber risk management by financial institutions (such as insurance companies and investment banks). The circular requires financial institutions to, *inter alia*, report to the Capital Market Supervisor and to the Board of Directors of such institution any significant cyber event that resulted in the unavailability of systems containing sensitive data for over three hours or if there is any indication that sensitive data was accessed regarding cyber risk management by financial institutions (such as insurance companies and investment banks). The circular requires financial institutions to, *inter alia*, report to the Capital Market Supervisor and to the Board of Directors of such institution any significant cyber event that resulted in the unavailability of systems containing sensitive data for over three hours or if there is any indication that sensitive data was accessed.

In addition, the Supervisor of Banks of the Bank of Israel ('the Banks Supervisor') published Circular No. C-06-2560 Re: Supply Chain Cyber Risk Management (24 April 2018) ('the Banks Supervisor Circular'). The Banks Supervisor Circular requires banks to, *inter alia*, report to the Banks Supervisor any cyber event that already occurred or any warning about a possible cyber event that may occur in the future.

JORDAN

Although Jordan does not currently have a data protection law in place, the country is taking steps to bring in legislation aimed at the protection of personal data. In 2014, the Ministry of Digital Economy and Entrepreneurship submitted a draft data protection bill ('the Draft Bill') which proposed, among other things, the establishment of an assigned council for the privacy commission. In addition, a committee consisting of different ministries, governmental authorities, and civil society organisations, was formed to discuss the Draft Bill. The Draft Bill appears to be based on the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and incorporates some of the main principles of the GDPR such as transparency, accuracy, storage limitation, and data minimisation. An updated version of the Draft Bill was published on 15 January 2020 by the Legislation and Opinion Bureau, however, a final version has yet to be approved.

LEBANON

While Lebanon does not have a comprehensive data protection legislation, privacy provisions are contained in Law No. 81 of 10 October 2018 on Electronic Transaction and Personal Data ('the Law'). This Insight provides an overview of the data protection regime in Lebanon.

Right of access

Article 99 of the Law states that data subjects have the right to inquire to the data controller about the processing of their personal data to determine whether his/her data is undergoing a processing activity.

In addition, the data controller must provide the data subject with a copy of the data belonging thereto at his/her request. In the case such data is encoded, compressed, or encrypted, the data subject must receive an understandable copy.

The data subject may also request the data controller, in accordance with the conditions specified in Article 99(2) of the Law, to hand over the following additional information:

- the purposes, categories, source, subject, and nature of the processing.
- the identity of the persons and their categories to whom the personal data is being sent, or those who can access the same; and
- the timing and purposes of such access.

In relation to the exercise of the right of access, Article 100 of the Law clarifies that the data controller may receive a payment for giving a copy of the personal data belonging to the data subject, provided that the payment does not exceed the cost of copying.

Moreover, the data controller may object to requests of an arbitrary nature, in particular with regard to the number of requests or their repetitive or systematic nature. In this case, when a dispute arises, the burden of proving the arbitrary nature lies upon the data controller.

MOROCCO

The Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data is inspired - to some extent - by European Union and French data protection law, as they both applied at the time when the Law was adopted. For example:

- Several of the Law's key concepts, such as 'personal data', 'processing', 'controller', 'processor', as well as several of its principles and individual rights, are identical or similar to that found in EU and French data protection law.
- Article 1 of the Law - which notably provides that 'computer is at the citizen's service and evolves within the framework of international cooperation. It should not infringe on human identity, as

well as collective and individual human rights and freedoms. It should not constitute a mean to disclose secrets from the private lives of citizens' - is close in its wording to the Article 1 of Act No.78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (as amended to implement the GDPR)

- The Law's material and territorial scope of application appears to be modelled on that of the Data Protection Directive (Directive 95/46/EC) ('the European Data Protection Directive').

There are also, nonetheless, important differences between the EU/French data protection law on the one hand and Moroccan data protection law on the other hand. One difference between these laws is that under Moroccan data protection law, consent is the main legal basis to process personal data in principle, and the other legal bases constitute exceptions to that principle. Under EU/French data protection law on the contrary, consent is only one legal basis among others, and legal bases are all considered on an equal footing (e.g., no legal basis is more important than the others)

PALESTINE[9]

Palestine, the issue is more complicated in light of the Israeli occupation, internal political turmoil and the Palestinian internal division. These factors led to the absence of a central authority responsible for regulating and protecting individuals' lives and privacy. With the absence of an effective legislative authority, there was a lack of structure causing a publicity of private data, and the ability of any party, whether official, private or security, to exploit the data of citizens present in the Palestinian territories. Palestinian laws, regulations and policies are still inadequate in terms of privacy, data protection and related electronic crimes, and the right to access information. This is what caused real problems worthy of evaluating the reality and proceeding with procedures and laws regulating all these developments, which this study seeks to discuss and research. This study aims to identify the reality of privacy and protection of personal digital data in Palestine, by surveying the mechanisms of data collection, how it is processed and its uses. Then, it presents the human rights violations that Palestinian users are exposed to regarding their personal data, in order to shed light on the basic features and principles on which the Privacy and Data Protection Law should be based.

TUNISIA

Organic Act No. 2004-63 of 27 July 2004 on the Protection of Personal details the scope of data protection and sets up a national commission in charge of its enforcement. For over a decade, Tunisian regulators have been trying hard to guarantee a high standard of protection of data for citizens. For this reason, several texts have been enacted such as the Law and Decree No. 2007-3004 of 27 November 2007 Laying Down the Conditions and Procedures for the Declaration and Authorisation of the Processing of Personal Data.

Law Reform

The Ministry of Justice was expected to propose a review of the framework for the protection of personal data, for the Law, by 2019. The review project of the Law has been under parliamentary scrutiny since 2017, however, the November 2019 parliamentary elections have delayed the review project.

[9] https://7amleh.org//storage/The%20Reality%20of%20Privacy%20Digital%20Data%20Protection%20in%20Palestine%20(1)_1.pdf

For the moment a new law project is still under the study of Parliament with collaboration of the National Authority of Data Protection ('INPDP').

5. PSD2 Implementation

5.1 The regulatory and institutional reform process

Payment Services Directive (PSD2) regulations were introduced to stimulate growth and competitiveness in the EU financial sector by simplifying the sharing of the infrastructure and customer data between incumbent banks and other players, including new financial institutions and fintech start-ups. This was driven as a top-down process, with the Council of the European Union passing the directive in November 2015 and giving member states two years to incorporate the directive into their national laws and regulations. This directive is administered by the European Commission´s Directorate General Internal Market.

For the definition and implementation of technical standards, between January 2019 and December 2021 the European Banking Authority established an industry working group to focus on the technical standards of APIs to be used under PSD2. A variety of external stakeholders joined this working group, chaired by the EBA. An equal number of nine representatives each came from Account Servicing Payment Service Providers (ASPSPs, essentially traditional banks and payment services companies), Third Party Providers (TPPs, these could range from new FinTechs to retailers like Amazon), and API initiatives, plus representatives from smaller standardization bodies, technical service providers and payment service users.[10] The working group was consulting to identify issues that emerged as the industry was preparing for the application data of the Regulatory Technical Standard on strong customer authentication and common and secure communication under PSD2, essentially the rules on the technical implementation of APIs for PSD2.[11]

The adoption and implementation Payment Services Directive 2 (PSD2) have radically changed the regulatory environment for providing payment services in the European Economic Area. Hence, beyond digitalization of basic banking services, Open Banking constituted a platform-based business approach where data, processes, and business functionalities are made available within an ecosystem of customers, third party developers, FinTech start-ups, or partners.

Payment Services Directive 2 (PSD2) enables access by non-banks to payments data in a way that previously only banks could do, allowing a much broader array of organizations to operate as Payment Service Providers. It additionally introduced enhanced security measures to be implemented by all service providers, including banks, which already had high security standards. This built upon the original payment services directive, (PSD) which provided the legal foundation for an EU single market for payments, establishing safer and more innovative payment services across the EU. The objective of the original PSD was to make cross-border payments as easy, efficient, and secure as 'national' payments within Member States. It offered economies of scale and helped the Single Euro Payments Area (SEPA), while providing more transparency and information for consumers.

To close this chapter, the major change here is that it is not only banks and traditional financial institutions who can see payment data, and that access to this payment data created a more vibrant and efficient financial services ecosystem that offers additional products and services to MSMEs and gives birth to a

[10] EBA WG-API under PSD2 - Industry participants list.pdf (europa.eu)

[11] EBA industry working group on APIs under PSD2 | European Banking Authority (europa.eu)

burgeoning FinTech industry that also is creating jobs. It can be expected that similar benefits could follow for the Southern Mediterranean if this path is followed.

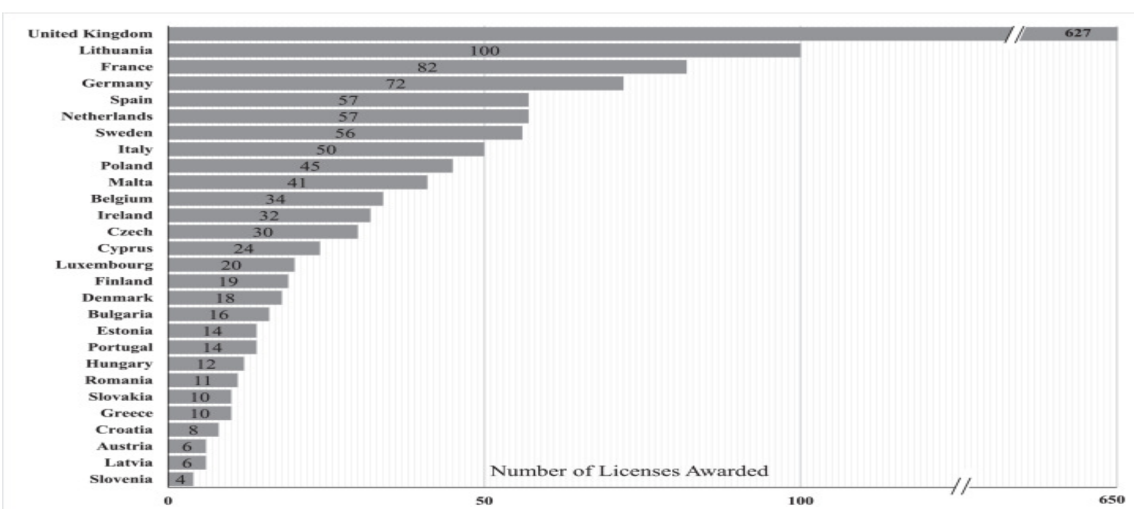
5.2 Description of Europe's experience with PSD2

The services provided are financial and may come from banks as well as from third parties. Adopting Open Banking regulations facilitated access to data has allowed banks and PSD2 licensed companies to tailor payment solutions and credit products to the needs of MSMEs and consumers who may have not met traditional credit risk criteria, and thus who would not have had access to finance.

Increased data about MSMEs and consumers allows banks to better know the payment histories of these companies and individuals, allowing not only banks but also new FinTechs and other non-bank financial institutions to begin offering credit products. Not only is there access to financial products where there may have been no access before, but there can also be competition in offering the best financial products to these newly creditworthy companies and consumers.

This sharing of data with the promise of financial innovation that would benefit all was not welcomed by everyone. Banks largely would have seen the proprietary value of the data they held about their customers as a big part of their value, and worried about the impact on the bank´s valuation of sharing these intangible data assets. As well, there was doubts on if the security standards proposed were going to be effective. With so much data to be shared via APIs, risks on data security, rather through cybersecurity weaknesses leading hackers to access data in APIs or misuse of data by external institutions are also concerns that needed to be mitigated. The latter, misuse of data by external institutions could also have been mitigated by Europe´s strong data protection rights under GDPR. In 2018, PSD2 was meant to shake the dynamics of the banking industry and pave the way to a new model of Open Banking. PSD2 is now considered a game changer and has expanded beyond retail banking. When a customer opts in, banks and other third parties will have access to that customer's current account data, which will enable an array of account aggregation and other open-data use cases. As opportunities to develop new products to offer consumers and MSMEs based on this current account data, demand for PSD2 licenses exploded, with 1,400 PSD2 licenses awarded as of only October 2020.

More than 1,400 PSD2 Licenses Awarded, as of October 2020, in Europe



Source: https://www.sciencedirect.com/science/article/pii/S0167268120302328

European digitalization movement developed bottom up following the financial crisis, starting with extensive reporting requirements, and creating the need for intermediaries and supervisors to digitalize, addressing initially specific concerns of financial regulators to better control systemic risks or of ensuring privacy in a world dominated by data-driven firms. The EU approach highlights that as financial systems digitize, it is necessary also to carefully consider approaches not only to financial regulation, but also to competition and data security and protection. Thus, Open Banking was pioneered in Europe in 2015 and was enforced in 2018 as a mandatory rule written in the PSD2 requiring banks to open their payments Application Program Interfaces (APIs – a means by which systems can electronically exchange and share data) to third parties.

Originally focused on payment services based on information from payment accounts, PSD2 provided two core services: 1) account information, and 2) payment initiation. With this regulation came several standards. These are the standards by which banking is effectively "opened" and democratized and financial innovation is spurred for the benefit of consumers. Open Banking is ultimately established when banks and financial institutions are required by regulators to enable Third Party Providers (TPPs) to access their platforms; whilst PSD2 regulations provide emphasized standards around authentication and communication, they do not provide by themselves technical standards for the API's which is the new element of the open finance which encompasses cross sectoral contributors. To move forward it was essential that all parties speak the same language and respect the "IT" limits, agreed upon in order to accelerate progress towards a truly open environment. The new directive therefore was designed to bring the financial market into the digital age, through both establishing a legal framework to better protect consumers while increasing competition, as well as establishing technological standards for these same purposes.

For this implementation to take place, new cybersecurity and authentication standards were also needed. Authentication is considered strong when it combines two of the following three elements:

- An element that only the customer knows (password, secret code, etc.)
- An item that only the customer has (mobile phone, bank card, etc.)
- A biometric characteristic (fingerprint, voice recognition, etc.). The opening of APIs will allow collaboration between incumbents and the Fintech ecosystem to use secure data and customer innovations to create new sources of revenue and services.

This authentication is necessary to protect data and that it is the proper person giving permission to use data.

5.3 A gradual Implementation

Finally, PSD2 regulators allowed an extension for companies to take 36 months to implement PSD2, as not all European countries are at the same level of implementation. As of a 2019 study by Deloitte, one can see clear differences in the level of implementation achieved throughout the European Union.

- ➢ The UK – a post-Brexit strategy to build a world-leading digital Open Banking ecosystem having set its own framework and API standards. Following CMA Open Banking commitments and PSD2 implementation, UK banks have transformed their proven payment infrastructure for Open Banking, while developing mobile immediate payment services based on the Faster Payments Scheme in a second step.

- France, Italy, Spain – Open Banking as a vehicle for digital transformation in domestic payment ecosystems
- Germany – a collaborative approach, specific to Germany, to the development of Open Banking. Germany's progress towards a full Open Banking environment can be characterized by the country's strong track record of cross-industry collaboration and innovation. The rollout of Open Banking in Germany has gained momentum. Intending to take advantage of pan-European developments such as PSD2 and SCT-Inst, German banks are in the stage of defining a digital strategy capable of delivering Open Banking payment services.
- Denmark, Norway, Sweden – the Nordic collaborative models and P27 initiative. By taking advantage of the Nordic collaborative models and pan-European developments such as PSD2, Nordic countries are transforming their payment infrastructure for Open Banking and have opened their respective mobile payment service schemes to other Nordic banks clients, in support of the pan-Nordic P27 initiative and the Nordic KYC Utility provider.
- Poland, Hungary – Open Banking as a vehicle for leapfrogging away from legacy banking infrastructures.

Deloitte 2019 study, reposted on Cloudoki

6. Why is PSD2 Important and how could it be implemented in the Southern Mediterranean?

PSD2 Directive is the regulatory constitution of a new business model, Open Banking. It is supposed to constitute an incentive to accelerate innovation in the payment services market and create new opportunities for FinTech start-ups. This will create increased access to credit, which is a major problem in the Southern Mediterranean region. Specifically, it is reported that only 8% of bank lending is availed to MSMEs[12] in the MENA region, although this population represents more than 95% of all corporate entities; in the EU Southern Neighbourhood, the annual financing gap is estimated to over hundred billion Euros (2018), most of which relating to the "SME" segment of the market, i.e., between 12 and 31% of the national GDPs.

[12] Improving access to finance for businesses in MENA region | World Economic Forum (weforum.org)

Out of the 5-6 million SMEs in the region, one third of them on average states that their growth is constrained by the lack of credit (up to 41% in Jordan and Palestine). It must be noted that these figures only translate the emerged part of problem: if the informal sector's financing needs were taken into consideration, this amount would be doubled.

The arrival of the Open Banking tsunami on the South Neighborhood shores is inevitable, so *it is advisable not to turn a blind eye on the PSD2, understanding the upcoming changes and reacting early will be key to yielding the best results.*

It should be noted that most banks in North Africa are in the process of changing and completely rethinking information systems towards global banking to international standards and therefore in accordance with the European payment directives PSD2, but there are varying degrees of strength and speeds at which countries and specific banks are making these changes.

MSME finance gap in NEAR in the Southern Neighbourhood

Key figures	ALG	EGY	ISL	JOR	LEB	MOR	PAL	TUN
SME Finance Gap (MLN USD)	No Data	46,722	No Data	6,582	5,676	31,479	No Data	6,874
Formal MSME Finance Gap as % of GDP	No Data	14%	No Data	18%	12%	31%	12%	16%
Informal MSME Demand for Finance as % of GDP	No Data	7%	No Data	5%	14%	22%	No Data	16%
Number of Formal MSMEs	No Data	2,454	No Data	156	171	1,410	171	601
Credit constrained MSMEs, % of total	No Data	33%	No Data	41%	36%	17%	41%	27%

Source: Study team based on data of IFC MSME Finance Gap (last updated in October 2018)

According to a survey in 2020 by the Arab Monetary Fund (AMF), the three main **use cases** PSD2 could make an impact in the region are for:

1) Credit transfers, and direct debits – influencing the development of the PayTech sector.
2) Going beyond payment accounts, e.g., loans, mortgages, credit cards, insurance, and investment.
3) Financial management (relying on limited payment data) with account aggregation which help manage cash flow to boost savings and earnings.

In general, the region depicts **prescriptive regulators** with binding standards more than moderators or market driven enablers, and cybersecurity is still viewed as the main challenge in implementation, still has precedence on customers engagement as main open banking's key perceived challenges, as well as meeting clients 'privacy concerns.

Most of region's central banks rate **financial inclusion** as their top priority for open banking. That prioritization reflects a shift toward seeing financially marginalized groups as an attractive proposition for financial services, mainly where traditional banks are not covering. And as much as it matters for unbanked individuals, better access to credit in the region matters much for small businesses. As a result, Arab countries will increasingly depend on open finance for financial inclusion and innovative financing for the small businesses that employ much of the population. The Arab region won't be unique in this regard, but the age structure of its population does provide it with an uncommon opportunity, as its young unbanked population, if banked, could lead to rapid growth in the banking sector.

A large concern about the implementation of Open Banking is the large portion of the population that remains unbanked, or not having access to mobile banking or digital banking services. Although traditional payment data can still be tracked and shared, if consumers are not using digital banking products, there is less space for financial innovation if FinTechs need to focus on non-tech financial solutions. However, were these consumers to obtain greater access to financial services and the ability to make payments digitally, this would represent an immense opportunity to financial institutions. The chart below shows a comparison of the countries in the region, with the United Kingdom as a benchmark, because it is one of the most advanced countries in implementation of PSD2.

Use of Systems and Tools that Facilitate Open Banking in Southern Neighbourhood

Key Figures	ALG	EGY	ISL	JOR	LEB	MOR	PAL	TUN	UK
Used the internet to pay bills in the past year (% age 15+)	2%	2%	38%	2%	6%	1%	No Data	3%	62%
Debit Card Ownership (15+)	20%	25%	38%	31%	35%	21%	No Data	23%	91%
Used a mobile phone or the internet to access a financial institution account in the past year (% age 15+)	2%	1%	47%	4%	5%	1%	No Data	4%	47%
Made or received digital payments in the past year (% age 15+)	26%	23%	91%	33%	42%	26%	No Data	38%	96%

Source: Study team based on data of World Bank Global Findex Database (last updated in 2017)

6.1 Comparison and measurement of policy and regulatory gaps

The policy and regulatory practices for each category and country of this studied were compared against the identified best practices and the magnitudes of the gaps were assessed using a simple colour mapping as shown below. This measured if the gaps were large enough to be important gaps, medium-sized gaps, or small gaps.

Important	Medium	Low	NA

It is important to highlight that the measurements of the magnitudes are to a certain extent subjective given the qualitative approach of this study and its subjects. Those countries marked in the lightest shade of blue have more steps to take before being ready for implementation of PSD2-style rules, while those in dark blue have a lower need for changes before implementing PSD2-style rules.

6.2 Overview of gaps of policies and regulations in the South MED region

Detailed Comparison of Policies and Regulations.)

Main Area / Country	**ALG**	**EGY**	**ISR**	**JOR**	**LBN**	**MOR**	**PAL**	**TUN**
Regulatory Framework								
Licensing								
National Settlement System								

Distribution Network								
Overall Ranking								

6.3 How can open banking be implemented in the South Mediterranean region?

These new services pose a challenge to the traditional model of Financial Service Providers (FSPs) operations because they allow external entities, or Third-Party Providers (TSPs), to obtain information, and initiate payments from consumer payment accounts operated by these FSP's. Therefore, external factors to be addressed comprise: technology developers, customers using financial services, and other financial institutions, and the legal environment in which these entities operate. Degrees of regulation should be dictated by market structure and cross-sector technological maturity; types of regulation should be influenced by distinctions between sectors and by the assorted roles of specific government agencies and self-regulatory organizations. Associated requirements for standardization will affect approaches to licensing, consent & privacy, user experiences, and operational specifications.

This is why we have noticed across the region disparities in the scope, depth and speed of progress which seem to be based on the following criteria:+--

(a) the market potential in the country concerned,
(b) the level of development of the payment system,
(c) the public environment for FinTech start-ups, including the regulatory framework.
(d) the authorities´ facilitation of innovation hubs and regulatory sandboxes for FinTech, which are also used as measures for the openness of the regulatory environment.
(e) the level of digital infrastructure,
(f) use of digital payments by consumers
(g) access to banking services (holding a bank account, credit card, or debit card)

Hence, the most important success factors perceived remain the creation of joint working groups to create promising use cases. MENA regulators considering Open Banking frameworks try to be inclusive, consultative, to listen to banks as well as FinTechs and consumers, and to be practical in how they develop this ecosystem. Based on the ideas from these working groups, Central Banks should act like Telecom regulators in order to be catalysts for transformation towards open banking. For this they must put dedicated teams, in order to put the rules in the following sectors: Legal, Strong authentication, API gateway standards, cybersecurity rules for banks and setting up sandboxes to test innovations and their compliance with standards. Initiatives to be proposed should also have a deadline as well for compliance; in Europe there was a deadline of three years for implementation.

In setting rules, it is important to determine which technical standards or codes of conduct the industry should adopt, particularly around enabling account access, prior to the full implementation of Open Banking i.e., prior to FSP's being required to enable API connectivity for TPPs. Developing decisions about which data should be accessed, cyber-security and customer consent, should not be a reason to put on hold the start of implementation of full Open Banking regimes and mandated API connectivity – that's also not how things developed around the world, and based on following rationale:

1- A principle-based implementation can increase efficiency relative to a prescriptive one (instead of specific rules, state the principles that guide bank´s actions).

2- Gradual expansion of functionality will ensure all stakeholders have sufficient time to address challenges (ex. Start by providing third-party access to account information services than to ask them to support third-party payment initiation services)

3- Standardization and Neutral Technology – common standards and technology will lead to greater efficiencies as financial data is shared, rather than a need for data to be ported from one unique system to another in order to be shared.

4- Level playing field fostering collaboration between stakeholders across different countries, which will help extend interoperability across the Arab region and help open banking makes connections with non-financial sectors and non-regulated players through open finance.

To further improve the regional fintech ecosystem, respective MENA countries may consider building strong bilateral agreements and cross-border collaboration initiatives with leading global hubs to benefit from knowledge, experience, and skills sharing, creating a more attractive and opportune market and ecosystem. On their own, most of these countries are relatively small markets, but if creating combined sandboxes where new solutions could be tested on a larger scale, there could be greater attraction of private sector innovators and even investment. Region-wide collaboration initiatives can be beneficial for all stakeholders across the region; the Arab Monetary Fund (AMF) is moving forward with the Arab Regional Payment System (ARPS) which would link payment switches throughout the region to enable cross-border large value transactions. This may allow further integration of sandboxing and licensing between member countries.

The enforcement of full Interoperability within a digital finance ecosystem encompasses three levels: (a) between financial institutions; (b) between all PSPs; and (c) between all cash-in/cash-out facilities. Effectively, PSPs tend to realize significant benefits of scale when fixed costs become relatively small and when there is complete interoperability at providers and at the market level.

7. Conclusion and Recommendations

PSD2 is being implemented in countries throughout the globe, and to not do so is to risk falling behind, as a result regulators are taking measures to develop policies allowing the utilization of this service. Those countries that develop strong privacy standards and APIs for sharing banking data will see a FinTech sector that can be complimentary to banks emerge, with increased access to financial services to MSMEs based on data sharing, and the creation of jobs as MSMEs grow eventually. Those countries without movement towards the PSD 2 concept will not only be able to develop the practical tools for their own domestic financial markets but will see innovative rivals from those countries eventually moving into their markets. It is understandable that traditional financial institutions see a threat, as new entrants to the market pose a challenge to the traditional model of Financial Service Providers (FSPs) operations by allowing external entities, or Third-Party Providers (TSPs), to obtain information, and initiate payments from consumer payment accounts operated by these FSP's. However, this research concludes that new FinTechs can also be complimentary to traditional financial institutions, allowing them to reach previously unbanked companies and consumers, provide more secured financial transactions and increasing the size of their revenues.

Moving forwarded, it is recommended to create national working groups who would evaluate the current financial sector policies and regulations, identify needs to develop the current financial system, strategize the implementation plan and find resources for implementation. These national working groups should include both public and private sectors such as banks,FinTech companies, consumers and MSMEs. This paper analyzes the gaps between what exists and what is needed for a PSD2 framework development working groups can build on this paper to discuss further the roles of specific government agencies as well as self-regulatory organizations and requirements for standardization such as approaches to licensing, legal, consent and privacy, user experiences and operations specifications (standardization of APIs, cybersecurity rules and the establishment of regulatory sandboxes). Once central banks or other relevant regulators have received sufficient feedback, they should act like Telecom regulators, acting as catalysts and making changes that will push the financial sector to the next level. Like in Europe, there should be a transitional period, so that there is time for proper technical standards to be set and implemented, and for governments to make any necessary legal or regulatory changes that are necessary before implementing these PSD2 rules that would bring Open Banking to the eco-system.

In setting rules, it is important to determine which technical standards or codes of conduct the industry should adopt, particularly around enabling account security and customer consent. However, the start of implementation should not be put on hold because of a delay in establishing technical standards or codes of conduct. Instead, there should be broad principles that guide banks and other financial institutions, instead of a prescriptive system in which specific rules govern each aspect of the institution's actions. Gradually expansion will originate, and new products can be offered, but the system can start simple, such as providing third parties access to account information first, then later allowing them to support third-party payment initiation services.

<u>Finally, an aligned approach should emerge from a flexible framework by incorporating a bottom-up approach to top-down regulation</u>. There are three models: 1) sandbox-based adjustments 2) transitional regulatory periods 3) alternative licensing arrangements. The latter is still not common within the South Med region, while the first two are becoming quite developed and well-funded.

To summarize, the next step should be creating national working groups from both public and private sectors to develop national strategies for adopting and implementing Open banking scheme. Using this paper as baseline and enhancing the public private dialogue can generate strategic vision to commence the regulatory changes, planning for a multi-year period in which standards can be clarified and new systems implemented.

8. Appendix 1: Individual Country Mapping

GAP Readiness mapping: This color coding shows if there is a significant or large gap between the rules in the European Union and the countries studied, a medium-sized gap, or a small gap between what exists in Europe and the studied country.

Important	Medium	Low	NA

8.1 EGYPT

Requirements / Approach	Regulatory framework	Licensing rules	National settlement system	Distribution network
Mandated and standardized	•	•	•	
Mandated and non-standardized				•
Market-driven and standardized				
Market-driven and non- standardized				

Egypt's open banking scene is gradually developing but still heavily **regulatory-focused** on enabling a comprehensive fintech ecosystem mainly targeting the unbanked, individuals and microenterprises informally operating.

Comprising 32 strategic initiatives, the CBE Fintech Strategy for EGYPT a cornerstone in this endeavor started in the second half of 2019 with critical initiatives targeted for completion by 2021 including a new banking law (September 2020) that allow the launch of digital banks. Main stated drivers are regulatory evolution, advancing financial inclusion, improve SME access to banking and financing, and support the transition to a digital and a cashless economy.

Egypt has issued its Personal Data Protection Law (15 July 2020), which is in line with the European Union's General Data Protection Regulation (GDPR). A Personal Data Protection Centre (the "Centre") oversees and enforces compliance with the Data Protection Law, while consumer protection and e-signature laws which have been enacted too will be fully enforced during 2022.

Finally, Egyptian parliament's CIT committee approved on November 29th 2021 the draft law regulating fintech for NBFI's under the FRA's authority which comes in line with the state's strategy to achieve **financial inclusion.** This important law is in line with the Financial Regulatory Authority Strategic Plan for the Development of the non-banking financial sector (2018-2022). The law aims at expanding the base of those who benefit from the non-banking financial services (NBFS), boosting the efficiency of NBFS, cutting the required costs of these activities, while allowing through metrics and AI a dynamic oversight of the sector.

8.2 JORDAN

Requirements / Approach	Regulatory framework	Licensing rules	National settlement system	Distribution network
Mandated and standardized	●	●	●	
Mandated and non-standardized				●
Market-driven and standardized				
Market-driven and non- standardized				

In its quest to overcome typical demographic challenges of its people such as the lack of access to financial services, gaps in identity documentation, and low financial literacy, the Kingdom capitalized on supportive regulatory environment and reliable telecommunication infrastructure to lead initiatives, following the 2017 launch of the National Financial Inclusion Strategy (NFIS) and the introduction of the Digital Finance Council (DFC), the Fintech Regulatory Sandbox. DFS is at the cornerstone of enhancements of the Jordanian government aims to address multiple issues, including simplified KYC procedures and basic bank account for excluded segments of the population, such as the low-income, women or refugees.

Jordanian market can thus fall within the category group of **digital smart followers**.

Payments and remittances are the predominant industries in line with e-commerce growth along with the established the Jordan Payments and Clearing Company (JoPaCC) to develop digital retail and micropayment systems and invest in innovative technologies CBJ has established a Regulatory Sandbox and introduced initiatives to include more vulnerable segments of society into the financial system CBJ expresses its continuous support for entrepreneurship in the Fintech sector and would like to open dialogue channels to sustain a consultative approach in order to support youth and entrepreneurs. In line with Central Bank's aim to be a fintech hub in the region, CBJ announced the establishment of a (Regulatory Sandbox). The Kingdom's ICT sector is dynamic, liberalized and well developed, contributing to the ecosystem.

Companies carrying out electronic payment and money transfer services activities in Jordan must comply with Instructions of Technical and Technological Requirements for the Electronic Payment and Money Transfer Companies No. (8 /2018); any third-party provider who wants to participate in open banking in Jordan needs to be approved by the Financial Conduct Authority (FCA) or a European equivalent.

In 2017, the CBJ improved the regulations by introducing "Instructions on the Protection of Personal Data of the Clients of Payment Services and Electronic Transfer of Funds" for non-banks to safeguard customers' money, to issue consumer protections rules, to develop customer complaints, to ensure systems governance and safety, and to develop data collection, analysis, and visualization

A draft data protection law (DPL) which will establish the Data Protection Council to regulate under the MoDEE is expected to come into force later this year to complement multiple laws and regulations earlier drafted for different purposes, which stipulate provisions on data protection pertaining to their respective scopes; ex. Banking, Telecom, Cybercrime.

8.3 LEBANON

Requirements / Approach	Regulatory framework	Licensing rules	National settlement system	Distribution network
Mandated and standardized	●	●	●	●
Mandated and non-standardized				
Market-driven and standardized				
Market-driven and non- standardized				

At present, Lebanon has not adopted an all-inclusive legal framework and digital strategy to lead the digital transformation in the Lebanese economy and govern fintechs or non-banks. Digital banking services are offered by traditional banks and licensed institutions by the Lebanese central bank which has issued a recent circular restricting to either banks, or NBFI's, the operation of e-wallets. Yet many private sector initiatives are planned in the purpose of enhancing and developing the fintech sector in Lebanon.

In application of Banque du Liban Basic Decision number 12872 dated 13/9/2018 on the General Data Protection Regulation (GDPR), and without prejudice to the mandatory laws and regulations applicable in Lebanon, banks and financial institutions operating in Lebanon and all other institutions regulated required to take the appropriate measures in line with the provisions of the General Data Protection Regulation (GDPR) promulgated by the European Parliament and the Council of the European Union on 27 April 2016.

No regulatory sandboxes offered to start-ups, limiting the degree of innovation, and increasing cost of failure. However, formation of Digital Committee in 2019 to map the structure and develop the governance of ICT, an affirmation of the strategic role of ICT in transforming the Lebanese economy.

Licensing is still complex and time consuming such as the 2018 law on electronic signature recently enacted, but which executive orders are still lacking.

8.4 MOROCCO

Requirements / Approach	Regulatory framework	Licensing rules	National settlement system	Distribution network
Mandated and standardized	●	●	●	
Mandated and non-standardized				●
Market-driven and standardized				
Market-driven and non- standardized				

In Morocco, the financial sector is regulated through the Moroccan central bank.

The protection of personal data has been regulated by law since 2011.

Commercial banks are powerful and agile and offer several services to their corporate clients. These banks encourage local Fintechs to make presentations and integrate the various innovations into existing banking systems.

There are 29 banks accredited with the Moroccan Central Bank, including 11 regional banks and 18 national banks. The largest of these banks include the People's Bank of Morocco, Ettijari Wafa bank, BMCE, TFBank and BEA.

In Morocco there are also offices of regional banks that operate in several African countries, such as the case of Ettijari Wafa Bank, which offer online services for all companies that export products or services.

Morocco additionally has about ten payment institutions, the largest of which are:
Barid Cash, Cash Plus, Damane Cash, Eurosol Cash and Quick Name.

The financial services innovation sandbox was placed by Mohamed 6 University, Polytechnic and several new services have emerged through Fintech.

The next step for the regulator, the Moroccan Central Bank, will be to regulate API access and security based on the PSD2 standard to industrialize all Fintech innovations across all banks at the same level.

8.5 PALESTINE

Requirements / Approach	Regulatory framework	Licensing rules	National settlement system	Distribution network
Mandated and standardized	●	●	●	●
Mandated and non-standardized				
Market-driven and standardized				
Market-driven and non- standardized				

Palestine has not elaborated a national strategy regarding open banking. There seems to be limited focus towards full-fledged FinTech development; as such, little or no implication of governmental bodies, with few measures introduced so far.

Priority has been given to reducing onboarding costs to consumers and enhancing accessibility, improvement of the distribution network through investments in Point-of-Sale (PoS) terminals. Furthermore, regulations allowing “mini branches” and agency banking and mobile money, are provided as to play a role in spurring adoption by increasing reach of financial services, while potentially reducing overheads and investment requirements.

Both MFIs and banks report to the supervision and inspection department at the PMA. Cooperatives report to the Ministry of Labor and thus are not considered formal providers of financial services. Other non-banking financial service providers are regulated by the capital markets authority.

8.6 TUNISIA

Requirements / Approach	Regulatory framework	Licensing rules	National settlement system	Distribution network
Mandated and standardized	•	•	•	
Mandated and non-standardized				•
Market-driven and standardized				
Market-driven and non- standardized				

In Tunisia, the financial sector is autonomous and very regulated through the Tunisian Central Bank. The landscape of open banking is being put in place with the efforts of each commercial bank, each of which tries to innovate by studying the offers of local Fintechs, which act on the Tunisian and European market.

The Tunisian central bank has launched a sandbox to test Fintech innovations mainly for the digitization of money, especially cryptocurrencies using blockchain technologies.

The country has 23 banks accredited by the Central Bank of Tunisia, the largest of which include BIAT, BT, UIB, UBCI, STB, BH, BNA, QNB and ATB.

Some commercial banks have started to open the APIs (Application Program Interface) for their customers, thus offering new online services, dashboards, account consolidations etc. The Fintechs hosted in the premises of the Tunisian central bank are discussing with commercial banks one by one which causes a lot of loss of time and adaptation of new innovations

The next step would therefore be to regulate and support innovations by implementing regulations inspired by PSD2 that protect and secure customers and APIs (Application Program Interface) in order to industrialize any innovation by giving free rein to competition between commercial banks.

Tunisia already has a data protection law and is in the process of validating a new law in accordance with the European GDPR.

The main obstacle found by Fintechs comes mainly from insurance payments that cover the risks in the event of fraud.

A law was passed in 2020 for the new method of financing companies through crowdfunding.

8.7 ISRAEL

Israel is in its own category regarding PSD2, as it has already implemented laws based on PSD2 in 2021, after draft proposals had been floated since 2016. Following PSD2, Israel will require banks and Israel will require banks and financial entities, with customer approval, to transfer customer information to technology firms who can provide customers with information about the financial services they consume, how much exactly they are paying and if they would save money moving to another provider. In testing the new financial reforms, Israel will establish a unique regulatory sandbox for FinTechs, where regulators can monitor them while they introduce new products into the Israeli market.

Israel already started work on the infrastructure for this system in 2019, working to build the required APIs following the Bank of Israel´s guidelines on the "Implementation of Open Banking," the first stage of which of this implementation strategy went into effect in April 2021 allowing access to be shared on account balances and transactions. A second stage is already in process to allow information on card transactions to be shared, and a third stage will involve access to data on a customer´s credit and loans, deposits and savings, and securities portfolio. This third stage is expected to be put into effect during 2022.

Israel´s banking sector is highly concentrated with two main banks, Leumi and Hapoalim, dominating the industry with a combined share of nearly 60% of total assets in 2020 and close to 70% of total consumer credit for the five largest banks. These banks, who have dominated the market for years, were opposed to reforms and have not yet seen the benefits of these reforms for them. A united front by government agencies overcame this opposition for the benefit of consumers as this regulatory system was created across government agencies with participation from the Justice and Finance ministries, the Securities Authority, the Bank of Israel, the Capital Market Authority, the Anti-Money Laundering and Terrorist Financing Authority and the Tax Authority.

9. Appendix 2: Acronyms and Terminology

- **PSD2** – Payment Services Directive 2
- **RTS** – Regulatory technical standards on strong customer authentication and common and secure communication (SCA and CSC)
- **ASPSP** – Account Servicing Payment Service Providers (often a bank)
- **PISP** – Payment Initiation Service Providers (third-party payment facilitator)
- **AISP** – Account Information Service Providers (third-party payment information provider)
- **TPP** – Third-Party Provider (a broad term to describe AISP's & PISP's)
- **PSU** – Payment Service User (consumers)

10. Appendix 3: Case Studies and Practitioners

Title: PSD2 for banks	Country: EU Member States
For banks, the new rules under PSD2 can potentially represent a threat to their business models. According to the EBA, most European banks continue to rely on large scale customised legacy mainframe IT systems (European Banking Authority, 2016). These systems are sometimes outdated and may not suit the modern digital environment (Oracle, 2011). Unless modernised, the antiquated bank IT will be unable to offer new services and will frustrate payment services users with long waiting times and a requirement to click through multiple windows. In this regard, the EBA also considers the entry of fintechs as both a challenge to and opportunity for European banks (European Banking Authority, 2016). In 1998, Microsoft founder Bill Gates expressed the challenge for banks, telling the United States Senate: "Banking is necessary, but banks – are not" (Gates, 1998). Investment in new API technologies will increase bank IT costs – and fuel competition which may cut into their revenues. They could lose 9% of revenue from retail payments to newcomers by 2020, according to IT services and software provider EVRY (Hafstad, et al., 2017). By 2025, some suggest that banks will lose more than a third of payment revenues to newcomers (Citi GPS, 2018). Some banks have concerns about providing open access to valuable payment account data without receiving anything in return. Although they recognise the opportunity to provide new payment services, Ana Botin, executive chairman of Spain's Santander, has spoken out on PSD2, arguing that banks should get access to fintech customer data to insure fair competition (Financial Times, 2018). More than fintech start-ups, banks worry about internet giants such as Apple and Amazon. While financial service start-ups often provide complimentary services, Botin argues that big tech companies threaten core bank operations. Internet giants have almost unlimited resources to access and analyse customer data, she says. The ECB recognises these fears but underlines that resistance among banks to PSD2 objectives only helps global giants increase their presence in Europe by constraining fintech enterprises (Mersch, 2018). As a result of PSD2, banks are creating proprietary API standards, allowing them to control access to payment account data. This might hurt fintech minnows, while failing to stop the internet giants who already own reams of data, says PPRO's Ralf Ohlhausen. According to a recent report by Deloitte, only a third of Central and Eastern European banks are at the stage of implementing PSD2. In Western Europe the share is somewhat higher, crossing the 50% threshold (Deloitte, 2018). Most are in a "wait and see" or "still evaluating" mode, the report says. They are leaving compliance to IT and legal teams, even though the regulation could lead to considerable strategic challenges in the payments market. "The figure is especially startling given that two-thirds of banks anticipate that PSD2 will affect all bank functions with numerous interdependencies with other regulations," the report warns. "The clock is ticking." Not all is black and white. Two out of three banks in a PwC survey "want to leverage PSD2 to change their strategic position" (Folcia & Firnges, 2017). This could represent even more innovation in the payment services market, representing increased competition for individuals and benefitting small businesses. About half of banks aspire to be what Price Waterhouse calls "a platform aggregator", allowing partners to integrate their services on the bank platform. All	

banks "need to analyse their products and services portfolio and determine their disintermediation risk for each product and service they offer".
Reference for the practices
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf

Title: PSD2 for Fintechs	**Country: EU Member States**
PSD2 is intended to spur competition by allowing fintech newcomers to provide innovative services. Newcomers already offer a wide range of financial services ranging from peer-to-peer investment to expense analysis and account overviews. Entrepreneurs and small businesses will attempt to incorporate 'security-by-design' into their products and practices. They will be under legal obligations to ensure protection of personal data (i.e., GDPR requirements). At the same time, businesses will try to avoid burdensome user experience that will slow down payments. For this reason, it is important that PSD2's mandated dedicated interfaces operate efficiently and smoothly. Under PSD2, start-up payment services providers will need to comply with rules for being either a Payment Initiation Services provider or an Account Information Services provider. Payment Initiation Services providers will be allowed to initiate payment operations while Account Information Services providers will be able to aggregate payment accounts data. At present, most rely on screen-scraping. A PSD2 mandated screen-scraping ban might limit access to data, resulting in two main challenges: • Each of Europe's 6,000 banks might develop different APIs, with different ways of connecting. Developers would struggle to keep up with this proliferation. • Efficient, fast, and stable connection must be guaranteed. Otherwise, connections could be cut off. Common technical standards could be one answer: the European Fintech Alliance has published a manifesto advocating the creation of unified pan-European API standards. At the same time, the Alliance wants to force banks to develop strong contingency measures if the API connection fails (The Future of FinTech Alliance, 2018).	
Reference for the practices	
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf	

Title: PSD2 for Consumers	**Country: EU Member States**
PSD2 is designed to help consumers by increasing both security and choice. By increasing security, consumer organisations believe PSD2 will increase consumer confidence in new payment methods. As evidence, they point to studies showing that consumer confidence in new online payment service providers remains weak. According to a report by Accenture, 76% of consumers rank the traditional bank as their first preference (Accenture Payments, 2016). In second place, the poll shows consumers prefer their online retailer to conduct the payment. Consumers are unhappy with the present payment options offered by banks. A CCG report shows that a majority of millennials are looking for new digital services, automatization and convenience (Schaus, Spataro, & Nguyen, 2016). Some 47% of respondents mentioned PayPal as their favourite payment method and only 6% use their bank's payments app. A majority seem to prefer convenience over security. Consumers want to make their purchases	

with a single click, as on Amazon's patented payment system. When asked to use a card reader or other device to buy a product online, vast numbers of consumers fail to complete their purchases, according to McKinsey (Hasham, Rezek, Vancauwenberghe, & Josh, 2016).
Reference for the practices
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf

Title: PSD2 for Regulators	**Country: EU Member States**
The European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) drafted both PSD1 and PSD2. Officials asked and received feedback from stakeholders and attempted to balance their interests. What the regulators failed to do was to create a strict Europe-wide framework. Each European Union member state must transpose the complicated rules, opening the door to fragmentation. National authorities will define what and how much bank data can be accessed. Penalties for non-compliance, exemption criteria, regulation authorities and other rules will differ from country to country. In other ways, too, regulators chose divisive compromises. After banning screen-scraping, they adopted contingency measures aimed at ensuring high-quality API standards for fintech companies. To address the subsequent complaints from banks, regulators followed up with criteria for exemption from contingency measures. The European Banking Authority added to the confusion by failing to give clear indications of exemption criteria: the consultation on the guidelines for exemption criteria started in June 2018 and no definitive statement has yet been made. In June 2018, the European Banking Authority consulted stakeholders to determine the list of key indicators and statistics required to ensure high-quality API connections. These guidelines are scheduled to be published by January 2019, two months before the beginning of the API testing period.	
Reference for the practices	
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf	

Title: PSD2 Adoption across Europe	**Country: EU Member States**
After PSD2 was approved, EU member states had two years to transpose it into national legislation. This period ended in January 2018. Yet only 17 of the 28 EU members have so far put the necessary legislation in place. According to the latest update from the European Commission (25 May 2018), four European member states have only partially transposed PSD2, while seven others are in the process of confirming drafts (Financial Stability, Financial Services and Capital Markets Union, 2018). Countries failed to meet the transposition deadline because of its complexity, because of its overlap with GDPR – and because in some cases, PSD2 contradicts existing domestic law. The Netherlands planned transposition to be completed by the spring of 2018. It missed the deadline, unable to decide which regulatory body is responsible for regulating bank APIs. Under current practices, the Dutch Central Bank, and the Dutch Financial Markets Authority share responsibility for regulating access to bank account information. This overlap of responsibilities create a legal ambiguity yet to be resolved by the government. The legislation is still in draft format before the Lower Parliament.	

Member states enjoy a large amount of flexibility when transposing PSD2. They are allowed to define the scope of payments accounts, determine the relevant regulatory bodies, and detail the registration process and penalties. Many regulatory differences exist between EU member states. For example, while France considers savings accounts come under PSD2, Belgium does not. The fragmentation may add to the complexities for small businesses doing cross-border operations, complexities the European Commission seeks to reduce with the Digital Single Market. Although legally obliged to transpose PSD2, countries do not face strict penalties if they fail to meet deadlines. The European Commission has launched infringement procedures over PSD2 against four member states, but the cases will take years to be decided by the European Court of Justice. Differences in national transposition could create operational complications for all stakeholders. Even though payment service providers are only obliged to obtain a license in a single European member state to operate across the European Union, the different national interpretations of PSD2 look set to fragment the market and may limit cross-border payment services.
Reference for the practices
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf

Title: PSD2 - Open Banking	**Country: United Kingdom**
The United Kingdom has moved ahead of the rest of the continent in payment regulation, implementing what it calls Open Banking. In its 2016 market research, the Competition and Markets Authority found that small and medium-sized enterprises suffered from a limited choice of retail banking and payment services (Smith, et al., 2016). Open Banking launched in January 2018, making it too early to deliver a definitive judgement on its success. Open Banking represents an innovative response aimed at stimulating competition. It is a private body funded by the country's nine largest banks, overseen by British regulators. Under Open Banking, the banks use a single common API standard – initially just for access to retail and business current accounts, though soon to be broadened out to cover all payment accounts. While smaller banks can install proprietary APIs, Open Banking motivates them to use the common APIs. Open Banking goes beyond PSD2, covering a wide scope of payment services. For example, it allows price comparison websites access to consumer current accounts. PSD2 does not. Early signs are encouraging Online bank Monzo has built its entire business on cloud services and applauds Open Bank's attempt to forge common APIs. "Although API is not the same as the UK standard, it is very similar," "It takes less than a day to configure for it." He likes the UK experiment because it insures that "our API standards are stable and will not change." For Open Banking to become a long-term success, common API standards are essential. Not all banks were ready to meet the January 1, 2018, deadline. Nine months later, some are still not able to deliver stable and fast access to accounts.	
Reference for the practices	
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf	

Title: The global race for digital payments	Country: China & US
While the UK imposes Open Banking and Europe grapples with PSD2, China and the USA are moving ahead to encourage payment innovation. In China, three quarters of online payments are done via mobile phone (Chen, 2017). In 2016, mobile payments expanded by 4.8 times over 2015, reaching 9 trillion US dollars. During the first ten months of 2017, mobile payments accounted for 16.7 trillion US dollars. Two internet giants – Alibaba's Alipay and Tencent's WeChat – dominate, with 55% and 37% market shares respectively (Chen, 2017). In China, mobile e-wallets are allowed to connect directly with bank accounts. This permits almost instantaneous payments, top-ups and withdrawals. The absence of a historic credit card infrastructure and the country's rapid growth of e-commerce are fuelling this mobile phone payment explosion. Until now, the government has taken a hands-off approach. Today, though, regulation is on the horizon. In 2017, the Chinese government created a nationwide clearing house for online transactions. It fears e-wallets may facilitate money-laundering. "The current direct connection model bypasses the central bank's clearing system, making it difficult for regulators to track and monitor the capital flow of those payments, leaving loopholes for money laundering and other irregularities," said Wang Pengbo, a Beijing-based consultant at Analysys (Zhang, 2017). Starting from June 30, 2018, digital payments must be routed through the centralised clearing institution. While China is coming to grips with the potential and threats of the growing digital finance sector, America lags behind. US mobile payments last year totalled a mere 112 billion US dollars, compared to China's 9 trillion US dollars (Carter, 2018). History explains much of the gap. Americans have long benefited from credit cards. Despite the emergence of new payment providers, from Paypal to Apple wallet, the vast majority of Americans continue to buy online with their credit or debit card (Stein, 2017). This credit card system is expensive. For each 100-dollar purchase, the merchant must pay 2.75 dollars to credit card providers and banks in fees. These fees total 90 billion dollars per year (Surane & Cannon, 2018). Strict regulation prevents the emergence of much digital payment innovation. A new payment provider in the US must often obtain state-by-state registration, apply for its own banking license or partner with an established bank. All these options are time-consuming and expensive. The Office of the Comptroller of the Currency has discussed the possibility of introducing a specific "fintech charter" (Skadden, 2016). State Bank Supervisors are working to unify their own regulatory requirements. If adopted, the credit card hold over US payments may loosen. With PSD2 and Open Banking, Europe enjoys an opportunity to leap ahead of the US in digital payments.	
Reference for the practices	
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf	

Title: Kreditech Case Study	Country: Poland, Spain
Background: Headquartered in Hamburg, Kreditech offers online consumer loans and an integrated financial services platform with custom-tailored products and services. Entrepreneurs Sebastian Diemer and Alexander Graubner-Muller founded the company in 2012. Since then, Kreditech has processed more than 31.6 million loan applications, 2.3 million	

of which it approved. It employs 350 people and operates in four markets. Kreditech's revenue more than doubled from 2014 to 2016, reaching €71.4 million in 2017. Business Model: Kreditech analyses a borrower's creditworthiness by examining their social network activity, browser history, and geolocation settings. Its algorithm customises the size of the loan and interest rate. This online credit search allows customers with little or no credit history to obtain loans, Kreditech says. PSD2: PSD2 could improve Kreditech's algorithm by allowing access to customer payment data. If banks provide low-quality API standards, it could be more difficult to produce the credit ranking. An absence of common European open banking standards will result in higher implementation costs. Kreditech worries about fragmentation. The differences in transposition across Europe could increase the costs of compliance. When asked about the legal ambiguity, co-founder Graubner-Muller replied. "It is yet to be defined and nothing is clear for the moment." Overall, Kreditech still treats PSD2 as more of an opportunity than a threat. Mr. Graubner-Muller believes "PSD2 will enable an easier switching between financial institutions and newcomers like Kreditech, and increase the transparency of the company's credit scoring"
Reference for the practices
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf

Title: PPRO Case Study	**Country: UK, Germany, Romania, Luxembourg…**
Background: Headquartered in London, PPRO is an alternative payment platform. It was founded in 2006 by Phillip Nieland and Tobias Schreyer. Since then, they have become one of the fastest-growing European fintech start-ups. It now employs more than 200 people and operates in several European countries. Activities: PPRO offers prepaid credit card payments and e-money accounts for consumers without credit cards. For merchants, it offers a wide range of alternative payment methods: real-time bank transfers, e-wallets and electronic cash payments. PSD2: The new rules will be key to the company's success or failure. In order to offer its payments solutions, PPRO requires access to customer bank accounts. It is participating in the API evaluation group and pushing for common pan-European API standards. Since such common standards are far from sure, Mr. Ohlhausen says his hopes that PSD2 will mean a breakthrough are "medium". Uneven transposition could still prevent market participants from developing a unified strategy for a single European market. "For some countries, PSD2 will be truly a step ahead in terms of innovation and access to accounts, as there was none before," he said. "For others, it will be rather a step back, since many countries had an advanced fintech regulation." Ohlhausen fears banks are not ready to comply with PSD2's data-sharing requirement and predicts that banks will be reluctant to provide high quality APIs. When asked who would benefit the most from PSD2, Ohlhausen responded: "the tech giants, followed by consumers and big retailers". Bank card payments will bear the biggest losses.	
Reference for the practices	
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf	

Title: Monzo	Country: UK
Background: Headquartered in London, Monzo is a challenger online-only bank. In April 2017, Monzo received a full UK banking license and is now able to offer current accounts. It was founded in 2015 by Tom Blomfield. By the end of 2017, Monzo had 750,000 current accounts holders and employed 275. Main activities: Monzo is a digital online-only bank. It does not have physical branches and does not provide chequebooks. All operations and transactions are conducted with a banking card or mobile phone. Before 2015, the bank could only provide pre-paid bank cards. These restrictions have been lifted and it now offers current accounts. The company plans to start offering loan products. PSD2: Under PSD2, Monzo is required to develop, implement and test secure communication API standards. Since Monzo is built on modern internet cloud services, it has an advantage over traditional banks who must deal with overhauling complex legacy systems. Monzo hopes the new standards might help it increase its competitive advantage and attract new clients. Even though Monzo now employs proprietary API standards, it favours common ones. "We will attempt to replicate the common standards as closely as possible so it would take less than a day to configure the connection," says Mr. Vans-Colina. Monzo already uses APIs to work with a dozen payment services. Low-cost money transfer firm TransferWise was the latest to join its platform in June 2018. A challenge is subscription renewal. Under PSD2, a customer is supposed to renew his or her subscription every 90 days. Otherwise, customers lose access to services offered by Monzo's partners. Monzo will implement an automatic re-subscription dashboard. "If confronted by regulators, we are willing to defend our views on this issue in open discussion," Simon added. Simon predicts PSD2 will lead to a large loss of market share for traditional banks. He expects them to fight access to customer data and to prove unable to innovate and offer effective e-payments.	
Reference for the practices	
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf	

Title: BBVA	Country: Spain, Belgium, France, Germany, Italy, Ireland, Portugal, and others
Background: Founded in 1857 and headquartered in Bilbao, BBVA is now the second largest bank in Spain with 14.8 million customers in 2015. In 2017, its revenue reached €25,270 billion. Main activities: BBVA is active in all banking fields including retail credit, capital markets, corporate loans and digital banking. In March 2015, Francisco Gonzalez, Chairman and CEO said: "Our goal is to turn BBVA into a totally digital company, including all our products and services" (González, 2015). The bank has created a special fintech-focused venture capital firm (Propel Venture Partners). PSD2: BBVA's digitisation plan includes development, implementation and testing of secure API communication standards. Mr. Hecht said BBVA will allow API access to bank accounts. While it could charge for such access in the past, it will offer it free of charge for now, in an attempt to get service providers to use its platform. When asked who would profit the most from PSD2, Mr. Hecht responded: "customers". With screen-scraping banned; he says they will enjoy enhanced security. Hecht criticised the fall-back mechanism, in effect allowing the use of screen-scraping under certain circumstances. In his view, screen-scraping is like handing out keys to an apartment. Under the fall-back	

mechanism, he says banks lose all control of customer data yet remain responsible for any security breaches. BBVA is determined to reduce its potential liability by developing high-quality API standards. It supports the PSD2 requirement for re-authentication every 90 days as a positive security feature
Reference for the practices
https://www.ceps.eu/wp-content/uploads/2018/09/RR2018_06_Europes%20Payments%20Revolution.pdf