Arab Regional Fintech Working Group

Open Banking Regulatory Principles

No.
164
2021

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and Monetary Authorities Governors

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
COUNCIL OF ARAB CENTRAL BANKS AND MONETARY AUTHORITIES GOVERNORS

صندوق النقد العربي
ARAB MONETARY FUND

Arab Regional Fintech Working Group

Open Banking Regulatory Principles

Arab Monetary Fund

March 2021

Acknowledgement:

This document was produced under the mandate of the Arab Regional Fintech Working Group (WG) mandate, The WG promotes the exchange of knowledge and expertise, strengthening the capacity of the Arab regulators, as well as building a network of Arab and international experts from the public and private sectors to promote the fintech industry and foster innovation.

The "Open Banking Regulatory Principles" paper was prepared by Samir Satchu of Algebra Advisors and Nouran Youssef from the Arab Monetary Fund.

Special thanks go to the Arab Central Banks and Monetary Authorities, members of the Arab Regional Fintech WG, in particular the Central Bank of Bahrain for providing their insights and comments on the policy paper.

Table of Contents

1. Introduction 5

2. Regional Developments in 2020 and 2021: Kingdom of Saudi Arabia and United Arab Emirates 6

3. Use Case for Emerging Ecosystem 9

4. Guiding Principles 11

Principle 1: Enable Locally Relevant Use-Cases to Emerge prior to the Full-Fledged Launch of Open Banking Regulations 11

Principle 2: Plan for Regulatory Mechanisms to Encourage Regulated Entity Take-Up within Set Timelines 11

Principle 3: Enable Permission Based Access Technologies Prior to Widespread Adoption of Open API Infrastructure in Order Not to Delay Innovation. 12

Principle 4: Drive the Early Adoption of Industry Standards on Regulated Entities & Certification of PISP/AISPs. 14

Principle 5: Ensure Robust Data Governance & Protection Frameworks are Applied by PISP/AISPs and Third Parties. 15

Principle 6: Require Consumer Protection & Liability Frameworks to be Adopted Across Open Banking Eco-Systems. 16

Principle 7: Actively Promote Early Industry Collaboration. 17

Principle 8: Adapt Phased Approaches to Reflect National Strategic Objectives and Use-Cases. 18

Principle 9: Broaden Scope & Regulate Not Only Banks. 18

5. Conclusion 20

Annex: Comparative Table on Open Banking Regulatory Frameworks 0

Abbreviations:

AMF	Arab Monetary Fund
AISP	Account Information Service Provider
API	Application Programming Interface
FIs	Financial Institutions
PSD 2	Payment Systems Directive 2
PISP	Payment Initiation Service Provider
TPPs	Third Party Providers

1. Introduction

The implementation of Open Banking regulatory regimes across the world, including Arab countries is accelerating.

Over the past year the Fintech Working Group has hosted a number of sessions with regulators and industry participants to share information on open banking models, and the benefits that open banking may generate for consumers in terms of increased competition and lower costs, innovation, and new use-cases.

There have also been significant open banking related regulatory developments in 2020 and 2021 in many Arab countries, namely the Kingdom of Saudi Arabia and the United Arab Emirates. This follows the Central Bank of Bahrain's launch of its open banking framework in 2018.

The objectives of this policy guide are three-fold:

(a) To present recent open banking regional regulatory developments in a global context;
(b) To set out some headline principles for Open Banking regulation; and
(c) To provide illustrative global Open Banking data points from a number of markets.

This policy guide has been drafted by the Arab regional Fintech Working Group with several primary considerations in mind.

First, Fintechs have a critical role to play in Open Banking as a source of innovation, since financial institutions and banks are not the only industry drivers in the Open Banking regulatory journey.

Second, locally relevant use-cases should be enabled early in the regulatory process, including before the establishment of regulatory frameworks in order to drive contextual regulation. Third, consumer protection should always be prioritized particularly with respect to data protection.

2. Regional Developments in 2020 and 2021: Kingdom of Saudi Arabia and United Arab Emirates

The classic Open Banking framework which has underpinned the development of many Open Banking regulatory frameworks around the world is that of the European Union (and to a lesser extent the United Kingdom) known as PSD 2 (Payment Systems Directive 2).

In its simplest form, PSD 2 is characterized by the imposition of a regulatory mandate on financial institutions to make their platforms and customer data available (within a specified time-frame and using an open API approach) in line with industry-wide standards to licensed third party providers that are acting on the express permission of end-users. We refer to this elsewhere as the "bank mandate".

At its core Open Banking is about two services (a) payment initiation – where a payment is initiated on behalf of an End-User and (b) account information services – where an End-User agrees to share their financial data with an authorized third party for, for example, expenditure analysis purposes.

In November 2018 the Central Bank of Bahrain adopted a broadly similar regulatory model mandating retail banks to give access to their "open API's" within 6 months, to licensed PISP and /or AISPs.

In 2020 several regulators started to establish frameworks that were intended in part to address Open Banking.

In KSA, Saudi Central Bank (SAMA) introduced payment initiation and account information services as payment services in the Payment Service Provider Regulations in Q1 2020[1].

In the UAE, the Central Bank introduced payment initiation and account information services in its draft Retail Payment Services & Card Scheme framework[2] – which has yet to be finalised. The Dubai Financial Services Authority amended its framework to allow

[1] https://www.sama.gov.sa/en-US/payment/Documents/PSPs%20Regulations%20111.pdf

[2] Pursuant to an industry consultation initiated by the UAE CB in November 2020.

for PISP and AISPs to be licensed in May 2020[3] and the Abu Dhabi Global Market initiated a consultation on such services in October 2020[4].

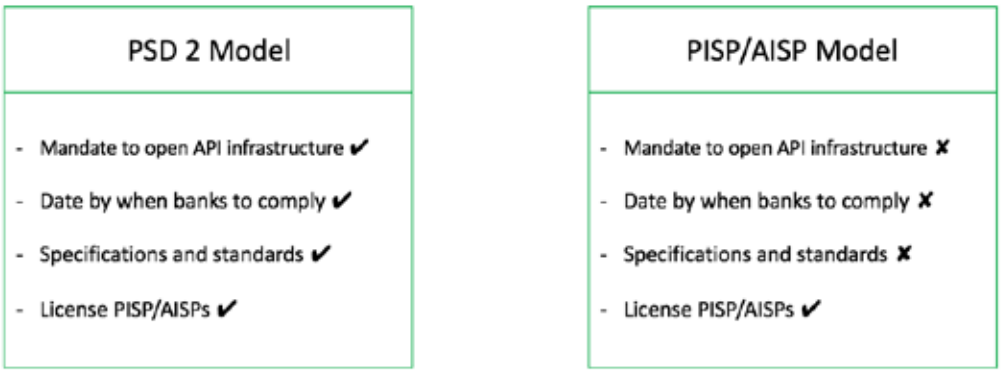
In Bahrain, the Central Bank issued its Open Banking Framework in October 2020, a framework intended to provide further clarity including across areas such as operational, customer experience, and security guidelines, governance and technical specifications.

Both the PISP and AISP regulatory framework under the Saudi Central Bank's Payment Service Provider Regulations (2020), and the emerging frameworks in the UAE are characterized by providing for the licensing of PISP and AISP but, importantly, without an adjacent requirement or mandate that is part of the PSD 2 framework obliging financial institutions to "open their platforms". In the case of the DIFC and the ADGM neither regulatory authority has jurisdiction to impose such a mandate on banks.

[3] https://dfsaen.thomsonreuters.com/rulebook/payment-service-provider

[4] https://www.adgm.com/documents/legal-framework/public-consultations/2020/consultation-paper-no-7/01-cp-7-of-2020proposed-regulatory-framework-for-providing-third-party-financial-technology-services.pdf

Diagram no. (1): Summary of Classic Open Banking Model vs "Bilateral" PISP/AISP Model



Note the characteristics in diagram (1) above are indicative of such frameworks only.

Typically, PISP/AISP frameworks do not contain time-lines for the opening up of API infrastructure or specifications and standards – instead banks and PISPs/AISPs are left to enter into bilateral contracts and agree specifications and standards.

In January 2021 the Saudi Central Bank released its Open Banking Policy. The Saudi Central Bank's Open Banking Policy sets out a 3 phased approach that contemplates the launch or go-live of Open Banking within KSA in 2022 following initial evaluation, design, and eco-system development phases to be undertaken in 2021[5]. As the licensing of PISPs and AISPs alone needs following progress to be a sufficient step to trigger the type of innovation typically associated with Open Banking. The more involved and holistic approach needs to be taken to ensure successful open banking outcomes.

[5] https://www.sama.gov.sa/en-US/Documents/Open_Banking_Policy-EN.pdf

Table no. (1): Summary of Regional Regulatory Developments on Open Banking

Market	Regulator	Development Summary
United Arab Emirates	UAE Central Bank	(1)Included PISP and AISP categories in its draft Retail Payment Services & Card Schemes Regulation (2) No bank mandate contemplated in draft RPSCS
United Arab Emirates	Dubai International Financial Centre	(1) DFSA includes PISP and AISP services as Money Services in updated framework in May 2020 (2) DFSA has no jurisdiction over banks in the UAE therefore no bank mandate possible
United Arab Emirates	Abu Dhabi Global Market	(1) FSRA released public consultation on in Q4 2021 covering PISP and AISP services. (2) Any FSRA regime will be similar to that of the DFSA – no bank mandate possible
Bahrain	Central Bank of Bahrain	Released Open Banking Framework in October 2020. Framework includes detailed operational guidelines, security standards and guidelines, customer experience guidelines, technical open Application Programming Interface (API) specifications and the overall governance framework needed to protect customer data
Kingdom of Saudi Arabia	Saudi Central Bank/SAMA	(1) Licensing of PISP and AISPs – Payment Initiation and Account information defined as Payment Services in Article 5 of the Payment Service Provider Regulations (PSPR). (2) No PISP or AISP licenses issued to date (3) No bank mandate in PSPR January 2021 – release of Open Banking Policy and full launch of Open Banking in KSA in 2022

3. Use Case for Emerging Ecosystem

The United Arab Emirates provides an important regional example and precedent of how Open Banking use-cases have emerged within an innovation enabling pre-regulatory environment.

Over the last 18 months a number of fintechs have started to launch payment initiation-based solutions in the United Arab Emirates prior (a) to the adoption of an Open Banking Regulatory framework and (b) prior to the wide-spread availability of Open Banking API infrastructure. As discussed elsewhere in this paper we believe that it is critical for regulators to enable the development of use-cases prior to regulating and using such use-cases as a base-cases for regulation as well as to enable innovation prior to the wide-spread availability of Open Banking API infrastructure.

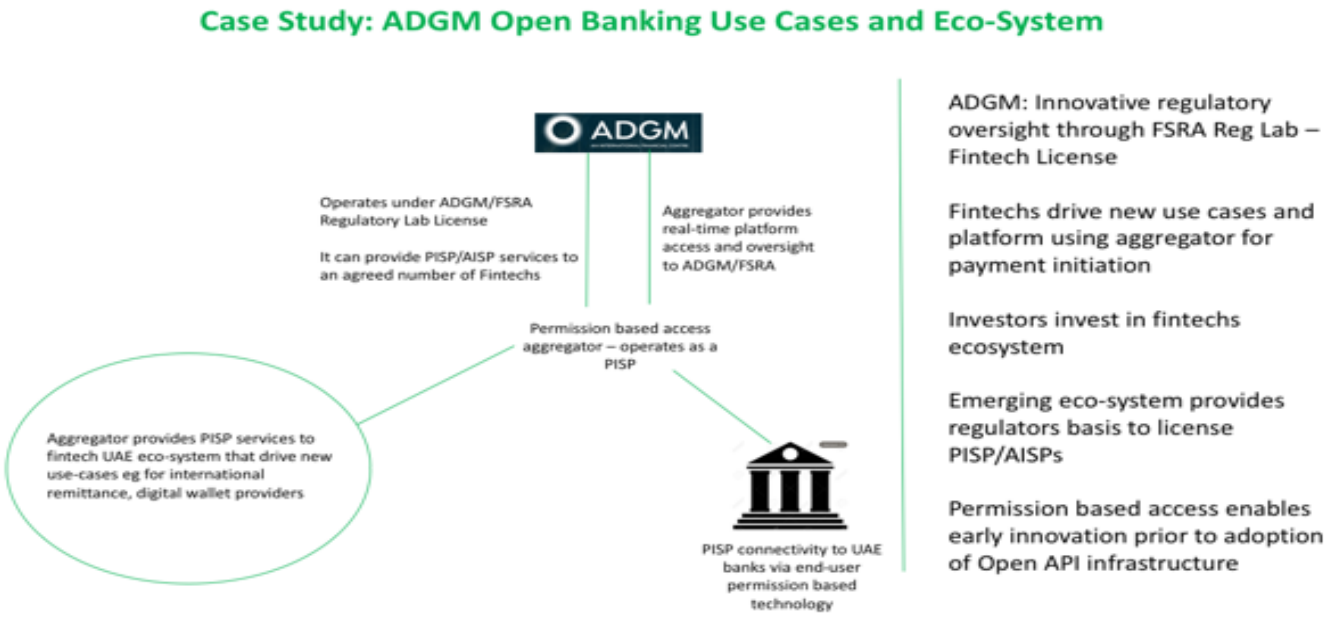
Of particular interest and worth noting in the UAE has been:

(a) the **emergence of locally relevant use-cases** based on local and market specific pain points such as payment initiation and international remittance;

(b) a **light and experimental regulatory license** issued by the Abu Dhabi Global Market and Financial Service Regulatory Authority's Reg Lab to enable experimentation whilst also ensuring real-time regulatory supervision of the eco-system[6]; and

(c) the UAE Central Bank's response to the emergence of the pre-regulatory Open Banking eco-system and its stated intention to license Payment Initiation Service Providers and Account Information Service Providers – **a regulator is regulating based on existing consumer activity and fintech participation in the market.**

Diagram no. (2): ADGM Open Banking Case Study



[6] The ADGM Reg Lab license issued to enable innovation in Open Banking type applications allow for a licensee to develop solutions with a limited number of fintechs to ensure managed growth whilst also ensuring that the FSRA has direct and real-time oversight over all transactional activity through its licensee.

4. Guiding Principles

Principle 1: Enable Locally Relevant Use-Cases to Emerge prior to the Full-Fledged Launch of Open Banking Regulations

National Open Banking Regulatory frameworks should be contextual, locally relevant, and based on evidence of market demand.

This is best achieved by enabling the early and pre-regulatory emergence of fintech ecosystems and use-cases which can be observed in order to better inform the regulatory process. This will permit regulators to define market relevant use-cases to build their frameworks around.

Principle 2: Plan for Regulatory Mechanisms to Encourage Regulated Entity Take-Up within Set Timelines

The PISP/AISP licensing model maybe be viewed as an Open Banking regulatory "half-way" house or interim step on a regulatory roadmap towards fully fledged Open Banking mandates. It allows for the licensing of PISP/AISPs without mandating the back end opening of financial institutions (FIs) platforms to those PISP/AISPs.

Under such frameworks the market (FIs and PISP/AISPs) is expected to reach bilateral agreements to deploy non-standardised access solutions.

However, **Regulated Entities (banks and other financial institutions) are under no obligation to meet timelines as none are set out under such regulatory frameworks**.

Whilst notionally "market-driven" such frameworks may lead to slower and more piece-meal adoption. Arguably, unless regulators enforce some obligation on Regulated Entities to work with PISP/AISPs to "grant access" on a "non-discriminatory basis" to TPPs financial institutions could impede innovation in Open Banking by slowing down the process by which they work with, and enable access for, PISP/AISPs, simply put by delaying concluding contracts with PISPs/AISPs or delaying deploying infrastructure to enable access to PISP/AISPs.

In Japan, the Financial Services Authority (FSA) imposed a dead-line of May 2020 by when Regulated Entities were to conclude entry into agreements with licensed PISP/AISPs. The FSA

had taken a hands-off approach and left commercial terms to be negotiated between Regulated Entities and PISP/AISPs which resulted in significant delays as terms could not be agreed.

In KSA, Regulated Entities are required to grant access to PISP/AISPs to Payment Accounts in "an objective, non-discriminatory and proportionate basis and in such a way as to allow the Payment Service Provider to provide Payment Services in an unhindered and efficient manner". It seems likely that, as PISP/AISPs enter the market in KSA, they may revert back to the regulator in the event that they are unable to get traction with respect to Regulated Entities granting them access in an objective and non-discriminatory basis. Note that the release of the Open Banking Policy with its emphasis on working with market participants in the design phase may be intended to address such concerns by encouraging early collaboration between and engagement with market participants.

Regulators should anticipate a second phase of engagement over implementation delays or delays in market adoption.

Examples of mechanisms to encourage adoption include:

(a) Setting out the commercial frameworks for bilateral agreements that Regulated Entities and PISP/AISPs should adhere to; and

(b) Requiring regular reporting on progress in terms of entry into agreements between Regulated Entities and PISP/AISPs.

Principle 3: Enable Permission Based Access Technologies Prior to Widespread Adoption of Open API Infrastructure in Order Not to Delay Innovation.

As stated above without the incorporation of mandates and time-lines on FIs there is a significant risk of delay. A solution that is intended to be market driven may result in slow adoption or market failure in the absence of wide-spread Open API availability.

Even where regulatory mandates have existed (e.g. under PSD 2), it has taken several years for FIs to establish PSD 2 compliant API infrastructure.

Diagram no. (3): Timelines

The European Union (and the Financial Conduct Authority in the United Kingdom) took steps to ensure that innovation continued during the three and a half year interim or transitional period towards widespread availability of Open API infrastructure.

Licensed PISP/AISPs were expressly permitted to operate and provide payment initiation and account information services using an End-User's credentials and permission and, in some instances, provided that the PISP/AISP identified itself to the Regulated Entity at the time of access. Such regulator approved access protocols are commonly referred to as Screen Scraping or Screen Scraping Plus and were permitted to be used provided that: (a) the PISP/AISP was licensed; and (b) the PISP/AISP had a valid security certificate which it would use to identify itself to the FI.

Screen Scraping is frequently dismissed out of hand – however, globally it has been the single most important driver of use-case development. It is important for regulators to be aware that such technologies (a) have been approved by best practice regulators in the EU and the UK prior to widespread availability of Open API infrastructure and (b) have been approved by financial services regulators on an on-going basis[7].

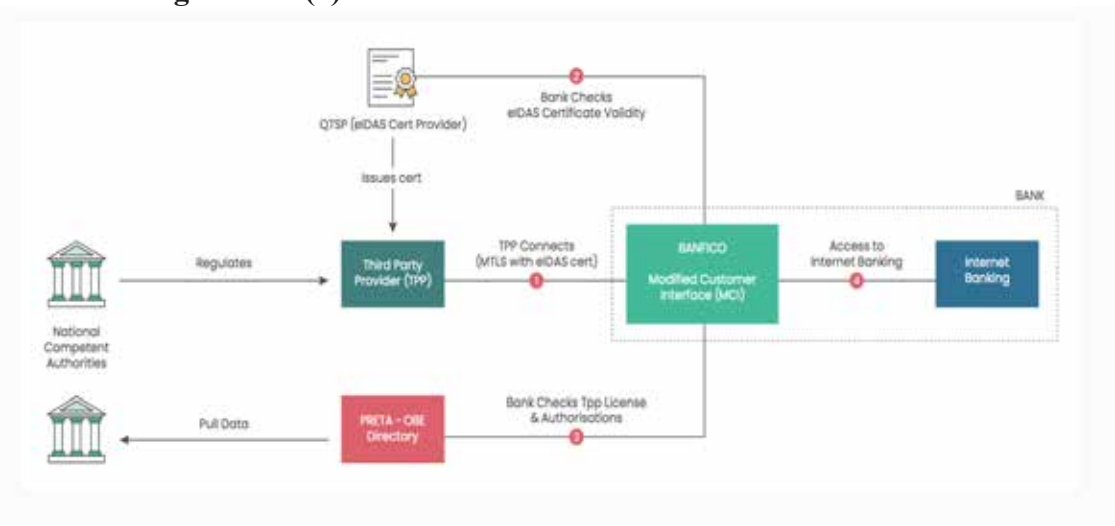
Whilst the ultimate goal and gold-standard is to enable open API access regulators have taken a risk-based approach with intermediate technologies such as permission based access as interim measures that balance the need for innovation with the need to ensure secure access.

[7] In March 2020 the Australian Securities and Investment Commission (ASIC) stated that it would not be restricting the use of screen-scraping techniques citing (a) a lack of evidence of any consumer loss from screen scraping and (b) arguing that it is a customer's right to decide who accesses their data.

The adoption and approval of such permission-based access methods when combines with licensing, security certification and identification has been critical to ensuring growth and innovation in pre-Open Banking regulatory environments or during transitional periods.

We believe that such global best practice is important for regulators adopting or considering both Open Banking regulatory models.

Diagram no. (4): Permission Based Access Architecture – EU



Principle 4: Drive the Early Adoption of Industry Standards on Regulated Entities & Certification of PISP/AISPs.

Notwithstanding the fact that under such a regulatory framework there is no regulatory mandate on Regulated Entities to open their platforms by a specified date, regulators should nonetheless ensure the early adoption of Industry Standards or Guidelines (including but not limited to technical standards, operational guidelines, customer guidelines, and security standards) that apply to any Regulated Entities that is opening its platform.

Such an approach reduces the high eco-system costs that will invariably arise if financial institutions open their platforms using a wide variety of technologies, platforms and standards. PISP/AISPs will not be able to scale if every integration is different. The benefits of Open Banking will be delayed not accelerated.

The fact that a framework is voluntary does not preclude a regulator from taking early steps to ensure early progress on harmonization of specifications and standards.

By way of example, the Monetary Authority of Singapore has been encouraging banks to adopt Application Programming Interfaces (APIs) since 2016 with the development of a financial API playbook despite not having publicly released Open Banking measures[8].

The development of standards need not be a top-down imposition by regulators. Instead regulators can consider requiring early collaboration within the industry to develop their own standards.

Moreover, in Nigeria a group of financial institutions and fintechs have come together prior to Open Banking being regulated to form Open Banking Nigeria and the Open Technology Forum, an industry non-profit whose primary objectives are to develop common API standards and promote adoption of Open Banking standards across all stakeholders in Nigeria[9]. In the United States, a market that is unregulated from an Open Banking perspective, the Financial Data Exchange[10], a non-profit alliance of stakeholders including financial institutions and fintechs emerged to unify the financial industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data.

Similarly, when licensing PISP/AISPs, regulators should require such entities to have their technology platforms certified for cyber-security purposes whilst also requiring licensed PISP/AISPs to adopt guidelines, policies and practices that address (i) strong customer authentication; (ii) dispute resolution; (iii) data protection and privacy; (v) insurance coverage; and (iv) consumer protection across the PISP/AISP eco-system.

Principle 5: Ensure Robust Data Governance & Protection Frameworks are Applied by PISP/AISPs and Third Parties.

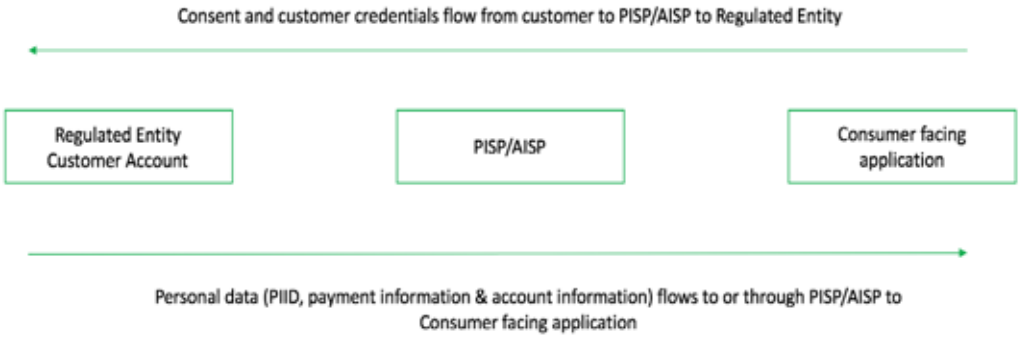
If Open Banking enshrines the principle of democratization of consumer-owned data it also necessarily relies on the development of robust data protection and data-use legislative and regulatory frameworks to allow for consent based sharing of data across Open Banking eco-systems, namely Regulated Entities, PISP/AISPs, and application developers.

[8] http://www.mas.gov.sg/development/fintech/technologies--apis

[9] See – www.openbanking.ng

[10] See – www.financialdataxchange.org

Diagram no. (5): Open Banking Data Eco-System



Regulators, often working with their peers in Data Protection Agencies will have to introduce approaches that ensure (a) consumer consent is always obtained prior to any data being captured (or payment being initiated); (b) data is only collected or used for the purposes for which consent is granted; (c) data is retained securely and in accordance with data protection and any applicable national residency requirements; and (d) that protect for data breaches. Unintended leaks or external attacks might expose customers' sensitive information, such as financial transactions and balances, bank account numbers or even online banking log-in credentials. In addition to violating customers' data privacy, the breach of personal identification can lead to identity theft, and subsequent financial losses for customers.

Where data protection principles are not embedded in national Data Protection legislation, regulators should consider whether data protection guidelines can be applied to PISP/AISPs as license conditions.

Principle 6: Require Consumer Protection & Liability Frameworks to be Adopted Across Open Banking Eco-Systems.

Similarly, with data protection, consumer protection frameworks need to be carefully applied when considering Open Banking regulatory frameworks. The Institute for International Finance[11] identifies three core areas which should be prioritized from a consumer protection perspective.

These relate to (a) unauthorised payments and (b) payment errors allocating fault between multiple players and (c) ensuring adequate and rapid consumer redress.

[11] https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf

Unauthorized payments or transactions made without the account holder's permission, can result from a data breach - but also from errors in (or attacks to) the functioning of payment initiation services.

Defective payments or transactions, requested by the customer but wrongly processed by the providers involved (due to mistaken amount or recipient, delayed timing or payment not executed) can also harm consumers if they are liable for charges from the intended payment recipients (e.g. providers or contractors of goods or services).

Diagram no. (6): Holistic Risk Management & Consumer Protection Framework

Table 1: EU Payment Services Directive (PSD2)

Authorization requirements for the third parties	• Governance arrangements and internal control mechanisms • Procedures to monitor, handle and follow up security incidents and security-related customer complaints • Processes to file, monitor, track and restrict access to sensitive payment data • Business continuity arrangements, including effective contingency plans • Security risk assessment and control and mitigation measures • Evidence that directors and persons responsible for the management are of good repute and possess appropriate knowledge • Professional indemnity insurance or some other comparable guarantee • *Only for payment initiation services:* evidence of an initial capital of at least EUR 50K
Rules on access to accounts and provision of third-party services	• Explicit customer consent • Limits on the access to, use and storage of customers data • Technical standards on authentication and communication, including mandatory strong customer authentication (i.e. two-factor authentication) • Limits on the access to accounts in case of unauthorized or fraudulent accesses • *Only for payment initiation services:* information for the payer and payee after the initiation of a payment order
Liability conditions	*Only for payment initiation services:* • In case of unauthorized, non-executed, defective or late executed payment transactions, the user shall obtain immediate refund from the account servicing payment service provider (i.e. the bank) and, then, if the payment initiation service provider is liable, this shall immediately compensate the bank • The burden shall be on the payment initiation service provider to prove that the payment order was received by the bank in accordance with PSD2 and that within its sphere of competence the transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency.

PSD 2 adopts a holistic approach to consumer protection and risk that encompasses:

(a) licensing, governance, and capitalization requirements for of PISPs/AISPs.

(b) requirement to obtain customer consent and customer authentication.

(c) clear rules and principles for burden of proof and resolution of payment disputes.

Principle 7: Actively Promote Early Industry Collaboration.

At its core Open Banking is about enabling access (to financial accounts and information) and facilitating greater competition. As such it is controversial and, as is often the case with any change that is perceived to be disruptive, has often been resisted by existing financial institutions or incumbents. That, as has been discussed above, frequently leads to delays in implementations.

The combination of a lack of awareness as to how financial institutions or incumbents generate value and financial returns on investment from Open Banking models drives hesitation and a lack of trust between industry participants, i.e. financial institutions, and fintechs.

From time to time industry participants should be strongly encouraged by regulators to form collaborative working groups at an early stage. This can be achieved through regulators signaling their intention to launch Open Banking frameworks and encouraging participants (through bank and industry associations) to collaborate as early as possible - as well as overseeing such collaborative initiatives. The Nigerian Open Banking initiative cited above is a good example of pre-regulatory industry collaboration between financial institutions and fintechs.

Principle 8: Adapt Phased Approaches to Reflect National Strategic Objectives and Use-Cases.

In many markets a phased approach to the implementation of Open Banking has been adopted with an initial focus on enabling data-based products. For example, in Mexico the Fintech Law (enacted in March 2018 but which came into effect only in 2020) sets out a phased approach to sharing data starting with the sharing of Open Data relating to ATM locations and service provider products and services. The Mexican Fintech Law does not provide for the provision of any type of payment services – a critical use-case of Open Banking.

Such an approach is restrictive (why and whilst cautious may be deemed to lack ambition and could miss opportunities in the payments space. Whilst "phasing" may be an approach worth considering, Arab country regulatory and supervisory authorities need not repeat data-only or data-first approaches but could focus on, for example, enabling a wider variety of use-cases across data aggregation and payments or use-cases that align with national strategic fintech priorities e.g. KYC or credit-scoring. Instead Arab regulators should consider payment initiation use-cases and base any phasing decisions on the types of use-cases that are emerging in their markets.

Principle 9: Broaden Scope & Regulate Not Only Banks.

The emergence and rapid adoption of non-bank digital wallet providers across the region means that there are many non-bank consumers of financial and payment services that can and should benefit from Open Banking initiatives. Accordingly, in markets which may have under-banked

populations and/or large segments of the population that utilize non-bank provided mobile wallets, such mobile wallet providers should also be considered Regulated Entities in order to make sure that Open Banking or Open Finance initiatives apply to as broad a segment of the population as possible. For example, In Europe PSD 2 applies not just to banks but also to e-money providers.

5. Conclusion

The implementation of Open Banking frameworks is at an early stage across Arab countries. There are lessons to be learned from the frequently delayed implementation of Open Banking regulatory models and the need to encourage innovation during such periods of delay. There are also lessons to be learned locally for example with rapid Open Banking implementations in markets like Bahrain.

As such regulators have a number of global and regional precedents that to base the development of their national frameworks on. The principles above, that are not intended to be exhaustive and have been extracted and summarized by members of the Arab Monetary Fund's Fintech Working Group, highlighting important regulatory framework considerations based on these global experiences in implementation and expectation of challenges particularly with emerging PISP/AISP licensing frameworks that are beginning to be adopted in the region.

As stated above the following core themes can be taken into consideration by Arab regulators when designing their Open Banking frameworks:

(i) **Enable innovation & use cases** to better inform regulation;
(ii) **Encourage early collaboration** in particular **around specifications and standards**;
(iii) **Contingency plan for implementation delays** including in API infrastructure availability;
(iv) **Ensure robust protection for consumers**.

For Open Banking to deliver value to consumers across Arab countries and promote competition, the most important pillar or guiding principle is to foster may be collaboration between Regulated Entities and PISP/AISPs.

Without that collaboration including to drive better understanding around the returns on investment on adopting Open Banking models and the adoption of common technical specifications and standards, it is likely that PISP/AISP frameworks may not deliver early gains for consumers that regulators are intent on driving.

ANNEX: COMPARATIVE TABLE ON OPEN BANKING REGULATORY FRAMEWORKS

Market	Framework Principles	Pre-Regulatory	Technology & APIs	Consumer Protection	Authorisation of TPPs
European Union	Payment Services Directive 2 adopted 8th October 2015 with 13th January 2018 set for commencement of applicability Defines two types of TPPs: - Payment Initiation Service Providers (PISP) - Account Information Service Providers (AISP) Together "Payment Institutions" Requires banks to grant payment account information access to authorised TPPs	FinTechs would either utilise screen scraping techniques or establish exclusive partnerships and custom integration with the banks A new form of screen scraping emerged under PSD2, called screen scraping plus. TPPs can still utilise the technique under a condition that they identify themselves to the banks through digital certificates	TPPs must comply with guidelines to ensure: - payment traceability - open and secure communication avenues for the customer - strong customer authentication - customers have personalised security credentials that are confidential - implementation of transaction monitoring mechanisms that avoid fraud APIs do not have to be standardised	General Data Protection Regulation (GDPR) dictates terms of consumer data access that TPPs are obliged to comply with Consumers must give "explicit consent to share their data" Data Protection Officers oversee compliance with GDPR Data subjects have ownership over their data Data subjects can ask for complete erasure of their data	Payment institutions must apply for authorisation through competent authorities of the EU member state

Australia	Consumer Data Right legislation commenced 6th February 2020 4 largest banks required to share consumer data with authorised TPPs by July 2020 All banks to provide access to financial data by July 2021 Opt-in service	FinTechs like TransferWise, Stripe, Airwallex, etc. have been present in Australia before the CDR - utilised screen scraping There are no laws that prohibit screen-scraping	TPP technology must comply with Consumer Data Standards: - Consumer Experience requirements - Consumer Experience guidelines - Information security profile (encryption, tokenisation) -API standards - Traffic expectations and data quality requirements	TPPs must have Consumer Data Right policy TPPs must implement 13 privacy safeguards as outlined under CDR TPPs must maintain records of collected data TPPs must submit reports to ACCC twice a year	TPPs must apply for accreditation through Australian Competition and Consumer Commission (ACCC) Foreign entities are required to have a local agent with an adequate insurance
United Kingdom	Competition and Markets Authority released an order for UK's nine largest banks to allow licensed TPPs access to financial data by January 2018 Differs from PSD2 in two aspects:	Credential sharing through screen scraping was common practice pre-OB Since 14 March 2020, TPPs must comply with the Secure Customer Authentication regulation, thus unregulated screen	UK operates on the Open Banking Standard principles, which includes specifications for: - APIs - Security profiles - Customer experience - Operational guidelines	UK participates in the EU's General Data Protection Regulation (GDPR)	1. TPPs have to apply for authorisation with Financial Conduct Authority 2. Enrol in the Open Banking Directory 3. Onboard onto the Directory Sandbox whilst waiting for applications to be processed

	- mandates common API standards across banks - uses a “whitelisting” approach for licensing TPPs	scraping is no longer allowed Licensed TPPs must identify them to ASPSPs in order to access consumer data			
Bahrain	Central Bank of Bahrain issued regulations on data sharing to be adhered to by all banks in the country by June 2019 Open Banking services are planned to undergo staged release, beginning with account aggregation, followed by payments	Screen scraping, although to a more limited extent, was practiced before regulation The practice is now forbidden under the Open Banking rules	Regulation sets forward standards for APIs, electronic identification, data transmission and web security	TPPs must maintain a secure customer authentication process for data access, aggregation and device access (biometric sensor) TPPs can opt for customised contracts with financial institutions to avoid fraud Customers must consent to initiate payment transfers	TPPs must be licensed under the Central Bank of Bahrain

United States	No explicit Open Banking regulation exists Financial Services Information Sharing and Analysis Center (FS-ISAC) has adopted the PSD2 standards to aid companies conducting transatlantic business Technically Section 1033 of the Dodd-Frank law guarantees the rights of individuals to access their financial data	Screen scraping practices are common in the FinTech industry Giants like Plaid, Venmo, Paypal and others operate freely in the US market			Bilateral or multilateral agreements on OB solutions are developed on a case-by-case basis

http://www.amf.org.ae

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and Monetary Authorities Governors