Arab Regional Fintech Working Group

Best Practices and Recent Developments for Digital Wallet Providers

No.
165
2021

صندوق النقد العربي
ARAB MONETARY FUND

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

Arab Regional Fintech Working Group

Best Practices and Recent Developments for Digital Wallet Providers

Arab Monetary Fund

June 2021

Acknowledgement:

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

The "Best Practices and Recent Developments for Digital Wallet Providers" report was prepared by Samir Satchu, Regulatory Advisor, Maher Loubieh from Hala corporation, and Nouran Youssef from the Arab Monetary Fund.

A special appreciation is extended to the Saudi Central Bank (SAMA) and other Arab Central Banks and Monetary Authorities, members of the Arab Regional Fintech WG, for their insights and comments that enriched the contributions to this report.

The Arab Monetary Fund
Economic Department, Financial Sector Development Division
Corniche Street, P.O Box 2818, Abu Dhabi, United Arab Emirates
Tel. +971 2617 1454
E-mail: Economic@amfad.org.ae; FintechWG@amf.org.ae,
nouran.youssef@amf.org.ae;
Website: www.amf.org.ae

The opinions expressed in this policy paper are solely those of the writers and do not necessarily reflect those of the entities they represent.

Table of Contents

Abbreviations

ADGM	Abu Dhabi Global Market
AML	Anti-Money Laundering
CAGR	Compound Annual Growth Rate
CFT	Combating the Financing of Terrorism
DIFC	Dubai International Financial Center
EMIs	Electronic Money Institutions
KYC	Know Your Customer
PSD 2	Payment Services Directive 2 (European regulation for electronic payment services)
PSPR	Payment Services Provider Regulations
SAMA	Saudi Central Bank
SBP	State Bank of Pakistan
SVEPS	Stored Value and Electronic Payment Services Regulation

1. Introduction

The on-going pandemic has increased interest amongst Arab countries in enabling and accelerating digital payments solutions across a range of sectors - thereby reducing physical transactions and reliance on cash.

Digital Wallet Providers (also known as Electronic Money Institutions) are a core component of the digital financial ecosystem both in terms of (a) facilitating fintech driven wallet solutions that address financial inclusion and (b) driving competition by introducing new entrants, new business models, new customer focused use-cases and digital experiences into the financial services sector.

The Digital Mobile Wallet market is expected to continue to grow significantly across the Arab region, including in the UAE at a compound annual growth rate (CAGR) of 12.7% to 2025[1]. In Saudi Arabia and Egypt respectively CAGRs of 18.2% and 19.3% are projected to 2025,[2]. These illustrative growth rates are above global averages of approximately 15% CAGR between 2020 and 2026.[3]

In other parts of the world, the rise of what is commonly known as "challenger banks" and new digital solutions was founded initially on enabling regulatory frameworks for digital wallet providers or electronic money institutions.

Such regulatory frameworks have been a building block and significant enabler for innovation and investment. For example, in the Kingdom of Saudi Arabia a number of diverse entities have recently been licensed, including STCPay, Hala, BayanPay, AlinmaPay, following the introduction of the Saudi Central Bank's (SAMA) Payment Service Provider Regulations (PSPR) in early 2020.

Accordingly, 2020 has seen a re-emergence of focus by some regulators in the Arab region on Digital Wallet Provider frameworks. This includes:

(a) KSA: SAMA's licensing of Major & Micro Electronic Money Institutions under the PSPR (2020)[4].

[1]Global Newswire, 2019. https://www.globenewswire.com/news-release/2019/11/13/1946577/0/en/United-Arab-Emirates-UAE-Mobile-Wallet-Payment-Market-Report-2016-2025-Market-Size-Forecast-Across-45-Market-Segments-600-KPIs.html

[2] Research & Markets, 2019. Saudi Arabia Mobile Wallet and Payment Market Opportunities, Databook Series. https://www.researchandmarkets.com/reports/4749478/saudi-arabia-mobile-wallet-and-payment-market?utm_source=BW&utm_medium=PressRelease&utm_code=jdfc6m&utm_campaign=1249671+-+Saudi+Arabia+Mobile+Wallet+and+Payment+Market+Opportunities+Databook+2019&utm_exec=chdo54prd

[3]Global market insights, 2019. https://www.gminsights.com/industry-analysis/mobile-wallet market?utm_source=GoogleAds&utm_medium=Adwords&utm_campaign=Technologies-PPC&gclid=EAIaIQobChMI2tHAoKD67AIVTe7tCh3R1AJQEAMYAiAAEgK2QvD_BwE

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

(b) UAE: The UAE Central Bank's launch of its new Stored Value and Electronic Payment Services Regulation (SVEPS 2020) earlier this month[5].

(c) UAE: A consultation being carried out by the Abu Dhabi Global Market[6] on revising is Money Service Providers regime as well as the revision of the Dubai International Financial Centre's framework for Money Service Providers[7].

In light of these recent developments the Arab Regional Fintech Working Group (WG) has drafted a summary of best regulatory practices for its members when considering regulatory frameworks for Digital Wallet Providers using, wherever possible, specific regional examples to illustrate the regulatory principle more clearly.

These principles are proposed by members of the Arab Regional Fintech WG and as such present an important basis for ongoing consideration of the optimization of national regulatory frameworks. The principles set out here are not intended to be exhaustive.

This paper represents the starting point for an extended exercise of analysis and engagement by the Arab Regional Fintech WG into Digital Wallet Provider frameworks and enablers which is intended to include engagement with, and feedback from, diversified stakeholders members of the group.

[5] The UAE Central Bank Stored Value Regulations (2020) are expected to be posted shortly on the UAE Central Bank website.

[6] https://www.adgm.com/documents/legal-framework/public-consultations/2020/adgm-fsra-consultation-paper-no1-of-2020-revision-of-regulatory-framework-for-providing-money-servic.pdf

[7] https://dfsaen.thomsonreuters.com/rulebook/gen-26-providing-money-services

Guiding Principles

Principle 1 – Enable Competition and Increased Digital Wallet Provider Participation by Direct Licensing of Digital Wallet Providers to Issue Electronic Money

Two main investment driven best-practice principles can be highlighted here:

(1) Direct Fintech Licensing and participation in the digital wallet eco-system.

Licensing vs Entry into Contracts with Banks (Bank-Led Model). Contrast Digital Wallet Provider frameworks in KSA, the UAE, Jordan, Bahrain, and Morocco for example where licenses are directly issued to Digital Wallet Providers against frameworks which, instead of issuing licenses to Digital Wallet Providers, require Digital Wallet Providers to enter into contracts with commercial banks to provide mobile money services i.e. and which restrict issuance of electronic money to commercial banks

Licenses are assets which Digital Wallet Providers are more likely to invest in over a bank partnership or commercial contract model where a commercial bank is the primary regulated entity and issuer of electronic money.

A Bank-Led Model creates uncertainty not only in the likelihood of the risk of termination of a fintech's contractual arrangements with a bank but also on business matters such as customer ownership i.e. whether under a Bank-Led Model the fintech fully owns the customer it provides services to, which may negatively impact business sustainability and financial performance. Such uncertainty when compared with direct licensing alternatives makes a jurisdiction less competitive when compared to jurisdictions which license Digital Wallet Providers directly.

Enabling the direct licensing and regulation of Digital Wallet Providers – as opposed to working through banks – results in a direct and more efficient regulatory relationship between regulators and Digital Wallet Providers and allows regulators to enforce regulatory requirements (e.g. across KYC, AML, capitalization) on Digital Wallet Providers rather than requiring partner banks to be an intermediary and/or the regulated entity for a business that is not ultimately theirs.

(2) No Imposition of Bank Ownership Requirements on Digital Wallet Providers

Regulators may consider requiring Digital Wallet Providers to enter into joint ventures with licensed commercial banks as a condition of licensing or operating in a jurisdiction. Imposing bank-ownership requirements on Digital Wallet Provider defeats the objective of enabling pure-play fintech participation, reduces a fintech's ability to generate returns from investments it makes, and results in delays as such joint ventures take time to structure.

Principle 2 – Digital Wallet Provider Capitalisation – Low Entry Point and Capital Linked to Size of Aggregate E-Money Balances

Imposing high initial capitalization costs for Digital Wallet Providers is a barrier to entry, fintech investment and innovation.
Developing best practice has adapted to provide for a Digital Wallet Provider's capitalization to increase in line with its size determined by the average e-money balances that are held by that e-money institution over a period of time.

Capitalisation structures for Digital Wallet Providers should reflect the fact that Digital Wallet Providers differ from licensed banks in two fundamental ways. First, they do not lend money and second, safe-guarded funds are held on trust with a licensed bank or in regulator approved securities. Imposing a high upfront paid in capital requirement is a blunt instrument when trying to encourage market entry by fintechs.

Instead of imposing high or fixed capitalization requirements on Digital Wallet Providers, regulators may consider (a) a combination of tiered license structures (e.g. for smaller and larger Digital Wallet Providers) and (b) capitalization requirements that increase in-line with the growth of a Digital Wallet Provider.

Principle 3 – Benchmark Capitalisation Requirements to ensure Competitiveness

Regulators are also encouraged to benchmark their capitalization requirements to ensure that they are in line with international, and in particular, regional markets.

Digital Wallet Providers will often base their investment decisions on comparisons between markets including with respect to capitalization requirements against market size and potential.

Please refer to table no. (2) p. 13, which illustrates the importance and value of capitalization benchmarking by comparing the impact of different capitalization requirements that are evaluated by a Digital Wallet Provider when comparing different markets.

Principle 4 – Define Payment Services Clearly and Expansively – Activity Based Licensing

Digital Wallet Providers are being enabled to provide digital payment services beyond the issuance of electronic money. The range of payment services should be clearly set out in definitions of "Payment Services" within regulatory frameworks.

Given the rapid expansion of the range of digital payment use-cases that are capable of being offered, clear definitions of permitted payment services that can be offered by Digital Wallet Providers provide clarity and should be expansively and expressly set out covering a broad range of payment services and as wide a range of possible use-cases whilst ensuring that regulators also retain the right to approve new Payment Services as innovative use-cases

emerge. Uncertainty over whether a use-case is permissible will lead to a delay in the launch of innovative use-cases in markets.

In particular, and as examples that have been highlighted through the Fintech Working Group we cite (a) the issuance of pre-paid cards without a bank as BIN sponsor and (b) non-bank merchant acquiring of transactions as examples of areas that would benefit from further clarification as regional examples of payment use-cases that have emerged from WG discussions.

Principle 5 – Allow for Innovative Agent Models

The scalability of agent networks with clear rules on agent liability and responsibility is fundamental to the success of Digital Wallet Provider eco-systems.

Specifically we consider that regulators should prepare for new types of agents and agent models, the enablement of super-agent networks (i.e. where a super-agent may recruit agent networks), whilst at the same time setting out clear guidelines and requirements for (a) how liability is assigned between Digital Wallet Providers and agent networks and (b) the scope of activities that can be carried out by agents (e.g. KYC, cash-in, cash-out, first line customer service).

Principle 6 – Limits & Balances

Best practice regulatory frameworks increasingly permit Digital Wallet Providers to set their own customer balance or transfer limits or have trended towards setting higher limits.

We recommend that Digital Wallet Providers be granted flexibility on limits setting so long as they adhere to robust KYC, AML, CFT and suspicious transaction reporting.

For instance, some jurisdictions do not impose any hard limits on Digital Wallet Providers, while reasonable limits may be set by Digital Wallet Providers given the existence of business justifications for such limits. Moreover, limits, where imposed, should be subject to an ongoing process of review and amendment by the governing authority/regulator.

Further and particularly in markets which have lower penetration of national ID documentation amongst their populations regulators should consider tiered or simplified KYC approaches which allow for the opening of Digital Wallet Provider accounts albeit with limits, for customers that do not have national ID or other KYC documentation.

Principle 7 – Enable Digital Wallet Providers to Generate a Return on Safe-guarded Funds & Require Diversification of Funds

It is an established and accepted regulatory principle that Digital Wallet Providers should safe-guard funds (a) in trust (or equivalent) with licensed banks and (b) segregate such funds from

operational funds and accounts. It is similarly well established that Digital Wallet Providers do not carry out the business of lending.

However, we consider that Digital Wallet Providers can be permitted to offset rising variable capitalization requirements linked to their size (i.e. the size of their aggregate e-money balances as stated above) by being able to generate some return through investing a portion of segregated funds in regulator approved return generating short-term securities.

Further as a prudential requirement and in order to mitigate risk we consider it appropriate for regulators to require Digital Wallet Providers to diversify safeguarded funds with multiple licensed banks upon such balances exceeding stated amounts to reduce the risk of a market failure linked to a bank that is holding safeguarded funds failing.

Principle 8 –Group Level Governance Structures and Graduation Path to Digital Banking

(1) Group Governance Structures

Digital Wallet Provider regulatory frameworks correctly emphasize governance structures and requirements for example, ensuring that certain management functions are established within licensed entities.

However, regulators may wish to consider the extent to which such functions may be provided through a centralised group function as opposed to locally.

In order to expand efficiently from one market into another Digital Wallet Provider groups, will frequently centralize certain business functions for example finance, technology or even audit and compliance. Here, the balance between efficiency and risk mitigations, which varies among countries, is also needed to be considered.

While centralised organization structures are crucial and important enablers for efficient scaling into multiple markets, the implication of such centralization on the local market need to be considered from regulatory and business perspectives. Arab regulators may consider governance requirements which prioritise organization design at a group level in addition to local level provided that regulators can at all times call on local representatives of licensed Digital Wallet Providers.

(2) Graduated Path to Digital Bank Licenses

For Arab markets which have licensed Digital Wallet Providers in an enabling way, it is advisable to consider the introduction of Phase two Digital Bank licensing frameworks noting that in markets such as the EU in particular consumer facing digital challenger banks or full-fledged digital financial service providers have typically emerged and graduated from being licensed first as Digital Wallet Providers or Electronic Money Institutions.

Principle 9 – Risk Management and Compliance Requirements

Digital Wallet Providers should adopt sound risk management frameworks, including policies, procedures and controls, to mitigate various types of risk such as operational risk; fraud risk; reputational and legal risks; liquidity risk; credit risk; counterparty risk; as well as market risk. The risk controls must be reviewed, and updated if necessary, on regular basis.

Similarly, Digital Wallet Providers should comply with the governing legal obligations and regulatory requirements for Anti Money Laundering and Counter Terrorism Financing (AML/ CFT), which implies establishing a proper compliance management scheme.

Moreover, Digital Wallet Providers should formulate robust data protection policies and measures in order to protect their information system and safeguard customers' data from any misuse and unauthorized actions.

Principle 10 – Cyber Resilience[8]

Digital Wallet Providers should employ suitable cyber resilience policies and strictly adhere to the cyber security provisions and obligations stated by the regulatory authorities.
Cyber resilience framework for Digital Wallet Providers should have the necessary consideration of various components, namely the cyber risk management components, including: Governance; Identification; Protection; Detection; as well as Response and Recovery.

Principle 11 – Customer Protection

Digital Wallet Providers should maintain vigorous operational framework to best serve the interest of their customers preventing their abuse, so that to ensure their promotional materials are clear, well understood, and not misleading. Moreover, all terms and conditions in addition to all terms of contracts should be clearly communicated and explained to the customers and in sufficient time. They also should provide their customers with clear, understandable, and easy to follow guidance on security measures.

Principle 12 – Corporate Governance Requirements

Digital Wallet Providers should have in place an appropriate corporate governance arrangement that ensure effective decision making and proper risk management. This might include among other requirements, a clear organizational structure with well-defined responsibilities, documented decision-making processes, controls on conflict of interests, as well as a code of conduct for both management and employees.

[8] Arab Monetary Fund, 2020. Cyber Resilience Oversight Guidelines for the Arab Countries, concerning Financial Market Infrastructures, March 2020. https://www.amf.org.ae/en/publications/cyber-resilience-fintech.

9. Regulatory References

Table no. (1): Regional Regulatory Precedents

Principle	Example
Enable Direct Fintech Licensing and Participation in the Digital Wallet Eco-System	The recent regulatory frameworks referred to in this paper (KSA, UAE Central Bank, DIFC, ADGM all provide for direct licensing of fintechs as Digital Wallet Providers. This builds on existing regional best practice and similar licensing frameworks in other AMF markets such as Bahrain, Jordan, Morocco, and Tunisia. The amended Egyptian Banking Law (2020) does not explicitly allow for Digital Wallet Providers to issue electronic money directly and outside of a Bank-Led Model but does allow for Central Bank of Egypt to directly license fintechs in Egypt.
No Imposition of Bank Ownership Requirements on Fintechs.	Under the UAE's prior regulatory framework SVEPS (2017) (Section E.2.2) (Ownership Requirements), licenses for the provision of full-service stored value and electronic payment services (Retail PSPs) could only be issued to entities that were majority owned (50%) by a UAE licensed bank. This provision has been removed from the UAE's SVEPS regulatory framework launched earlier this month – probably in response to the fact that such partnerships may be complex and time-consuming to structure and were a disincentive to fintech participation and investment when compared to other markets where similar restrictions do not exist.
Digital Wallet Provider Capitalisation – Low Entry Point and Capital Linked to Size of	KSA: Low Capitalisation Entry Point: SAMA's PSPR (2020) create 2 categories of Digital Wallet Providers to enable market entry of smaller players. Under the PSPR there are two categories of Digital Wallet Providers (known as Electronic Money Institutions) - Micro EMIs and Major EMIs. Micro EMIs are restricted to Total Average Outstanding Electronic Money balances of (SAR 10m) and/or Average Monthly Transaction Value (SAR 10m).

Aggregate E-Money Balances	Major EMIs have to maintain 2% of the Total Outstanding Average Electronic Money – i.e. the total value of the electronic money issued by the Digital Wallet Provider. UAE: Under the UAE's new SVEPS (2020) framework initial capitalization requirements have been reduced from what was perceived to be a high entry point of AED 50m to AED 15m with an on-going capital requirement of 5% of Average Capital Funds.
Define Payment Services Clearly and Expansively	KSA: Building on the European Union's PSD 2 framework, KSA's framework under the PSPR is notable in 2 respects: (1) In setting out that Major EMI's can offer one or more Payment Service - in addition to issuing electronic money; and (2) Defining Payment Services clearly to include, for example, Money Remittance, Acquiring Transactions, and the Issuance of Payment Instruments such as cards The KSA PSPR (2020) also include Payment Initiation and Account Information Services as Payment Services that can be provided by Digital Wallet Providers – one of the first such regimes in the region alongside the Central Bank of Bahrain, and the Dubai International Financial Centre to recognize open banking services as services that can be provided by Digital Wallet Providers in KSA. SAMA's framework states that (Article 6.5): A Major EMI must issue Electronic Money as an e-wallet (and may, if it so chooses, carry on one or more of the Payment Services permitted for a Major Payment Institution). SAMA defines Payment Services as follows: (a) the execution of Payment Transactions, including (A) transfers of funds on a Payment Account with the Payment Service User's Payment Service Provider or with another Payment Service Provider and (B) where the funds are covered by a credit line, and: (i) the execution of Credit Transfers, including Standing Orders; (ii) the execution of

	Direct Debits, including one-off Direct Debits; and (iii) the execution of Payment Transactions through a payment card or similar physical or digital device; (b) issuing Payment Instruments; (c) issuing Electronic Money (by opening e-wallets or otherwise); (d) Acquiring Payment Transactions; (e) Money Remittance; (f) services enabling cash to be placed on or withdrawn from a Payment Account and the operation of a Payment Account; (g) Payment Initiation Services; (h) Account Information Services; and (i) any other activity designated by SAMA as a Payment Service.
Allow for Scalability & Innovation in Agent Networks	Pakistan: As an example of an innovative and forward thinking approach to agent networks we cite the State Bank of Pakistan's (SBP) inclusion in its Regulations for Electronic Money Institutions (2019)[8] a definition of agents that referred to them as "static or movable". SBP provided for "movable agents" specifically in response to the rapid growth of app-based ride-hailing services in Pakistan such as those provided by Uber and Careem and in order to try and enable such companies to use their drivers as agents and providers of mobile financial services for cash-in and cash-out services. Further, and as sign of its intent on enabling provision of agent services by micro SMEs and individuals, SBP did not require that an agent be a legal person instead choosing to define agents as: "*a natural or legal person*, non-bank and non-EMI outlets, *static or movable*, who can provide payment services as well as distribute and/or redeem e-money on behalf of an EMI under a valid agency agreement".

[8] https://dnb.sbp.org.pk/psd/2019/C1-Annex-A.pdf

	It is also worth noting that there is no requirement for a regulator to approve an agent. Agent approval may take time. Instead regulators should consider imposing requirements which Digital Wallet Providers are required to comply with.
Limits and Balances	UAE: See Article 13 (Schemes & Operating Rules) of the UAE Central Bank's launch of its new Stored Value and Electronic Payment Services Regulation (SVEPS 2020). The framework does not impose any hard limits on Digital Wallet Providers instead stating that reasonable limits may be set by Digital Wallet Providers provided that there are business justifications for such limits. The limits are subject to the ongoing review and amendment of the Central Bank. KSA: There are many provisions, which depend on the license types and conditions. For instance, article 6.5 of the SAMA PSPR (2020) allow for single account limits of SAR 100,000 and place a monthly transaction limit of SAR 100,000 on transfers to and from a Digital Wallet Provider account.
Enable Digital Wallet Providers to Generate a Return on Safeguarded Funds	KSA: SAMA clearly allows for the investment of safeguarded funds in approved securities by SAMA as being secure and liquid. The SAMA framework states that if a Digital Wallet Provider "wishes to invest the Safeguarded Funds, the assets in which it intends to invest must first be approved by SAMA as being secure and liquid".[9]
Diversification of Funds	Diversification of Safeguarded Funds: To mitigate risk further by diversification, State Bank of Pakistan introduced a requirement whereby a Digital Wallet Provider holding in excess of a prescribed amount in safeguarded funds would be required to diversity such additional amounts with more than one bank. SBP's Regulations for Electronic Money Institutions state "EMIs shall not place more than 50% of e-money balances with one Trustee in case its outstanding e-money balance exceeds PKR 100 million."[10]

[9] Article 14.2 (2) of SAMA'S PSPR (2020).

[10] Article 14 of SBP Regulations for Electronic Money Institutions (2019).

Table no. (2):

The table below illustrates the importance and value of benchmarking by two markets for a Digital Wallet Provider – to illustrate we have assumed the Digital Wallet Provider has the equivalent of USD $100m in average outstanding balances.

Markets	A	B
Population	10m	30m
Paid in Capital	USD $5m	USD $3m
Variable Capital – assuming USD $100m	5% of the Average Capital Funds = USD $5m	2% of Total Outstanding Average Outstanding Electronic Money = USD $2m
Capitalisation Requirement	USD $10m	USD $5m

When compared the capitalization differences between similar sized businesses are significant particularly when taking into account differences in population.

Conclusion

As mentioned earlier, the principles set out in this paper have been worked on in collaboration within the Arab Regional Fintech WG. They include feedback from Digital Wallet Providers but also reflect recent developments in 2020 in various Arab regulatory regimes including the Kingdom of Saudi Arabia and the United Arab Emirates.

Digital Wallet Providers - and fintechs more largely – generally prefer to be directly licensed and regulated. Relying on banks as exclusive issuers of electronic money might impede stand-alone Digital Wallet Providers investing in a market as is requiring bank participation in other forms – namely as equity participants with fintechs. Such restrictions are being eliminated in the region as evidenced by the UAE Central Bank's removal of such requirements in the framework announced earlier this month.

Similarly, high initial capitalisation requirements, where recent regulatory developments highlighted in this paper demonstrate that regulators are moving away from high and fixed up initial capitalization requirements towards variable requirements linked to size which is a positive development. Nonetheless regulators need to be acutely aware of the fact that their frameworks need to be competitive within the region to attract investment and participation by new entrant Digital Wallet Providers.

Moreover, Digital Wallets Providers shout adopt set of Risk Management and Compliance Requirements including a proper compliance management scheme for AML/CFT frameworks, and formulating robust data protection policies and measures.
They should also employ sound cyber resilience policies, including cyber risk management components, and strictly adhere to the cyber security provisions and obligations stated by the regulatory authorities.

Digital Wallet Providers should maintain vigorous operational framework to best serve the interest of their customers preventing their abuse on many fronts, e.g. their promotional materials, terms and conditions, terms of contracts, as well as guidance on security measures; to be clearly communicated and explained to the customers and in sufficient time.

It is crucial for the effective decision making and proper risk management that Digital Wallets Providers put in place an appropriate corporate governance arrangement, with clear organizational structure, well-defined responsibilities, documented decision-making processes, controls on conflict of interests, as well as a code of conduct for both management and employees.

للحصول على مطبوعات صندوق النقد العربي

يرجى الاتصال بالعنوان التالي:

صندوق النقد العربي

شبكة المعرفة

ص.ب. 2818

أبو ظبي- الإمارات العربية المتحدة

هاتف رقم: 26215000 (971+)

فاكس رقم: 26326454 (971+)

البريد الإلكتروني: Publications@amfad.org.ae

متوفرة إلكترونياً بموقع الصندوق على الإنترنت: www.amf.org.ae

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