DEVELOPING DIGITAL PAYMENT SERVICES IN THE MIDDLE EAST AND NORTH AFRICA

A Strategic Approach

WORLD BANK GROUP

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

DEVELOPING DIGITAL PAYMENT SERVICES IN THE MIDDLE EAST AND NORTH AFRICA

A Strategic Approach

WORLD BANK GROUP

TABLE OF CONTENTS

FIGURES, TABLES, AND BOXES

FIGURES

TABLES

BOXES

ACKNOWLEDGMENTS

The lead author of this report is Biagio Bossone, external expert. Holti Banka (Financial Sector Specialist) collaborated on data and statistics, Arpita Sarkar (Consultant) provided support and inputs, and Harish Natarajan (Lead Financial Sector Specialist) provided overall guidance and supervision. The team would also like to thank Mario Guadamillas, Djibrilla Issa, Georgiana Pop, and Gonçalo Coelho for providing valuable comments as peer reviewers. The team is also grateful to Nadir Mohammed, Mahesh Uttamchandani, Irina Astrakhan, Onur Ozlu, Daniel Lederman, and the World Bank MENA Chief Economist Office.

ACRONYMS

ACH	automated clearing house
AML/CFT	anti-money laundering and countering the financing of terrorism
CDD	customer due diligence
DFS	digital financial services
DPS	digital payment services
FPS	fast payment system
GCC	Gulf Cooperation Council
KYC	know your customer
MENA	Middle East and North Africa
MNO	mobile network operator
NPS	national payment system
POS	point of sale
PSP	payment service provider
RTGS	real-time gross settlement
SME	small and medium-size enterprise
UAE	United Arab Emirates

EXECUTIVE SUMMARY

This report has been prepared to inform the ongoing MENA Tech program and is directly linked to the cashless payments Marrakesh 2021 targets. The objective of the MENA Tech program is to help World Bank Group teams and external stakeholders achieve regional priorities for digital transformation of government and the economy and regional integration, with a particular and initial focus on reaching the Marrakesh targets for connectivity and cashless payments. MENA Tech aims to achieve this by providing analytical tools, including frameworks, data, analytics, and knowledge-exchange opportunities to operational teams, clients, and regional stakeholders.

This report discusses strengthening the provision of payment services in the countries of the Middle East and North Africa (MENA) region as an essential step to integrate their economies into the world of "digital finance and digital economy" and to support economic development. The report elaborates a strategic approach to the development of sound and dynamic ecosystems for the provision of digital payment services (DPS) as foundations for effective financial digitalization and development of digital economy in MENA countries. The report is not about intervening in the MENA region through a coordinated regional strategic plan; rather, it describes what MENA countries should do in order to modernize their DPS ecosystems, starting from their own initial conditions. To this purpose, it identifies steps that are tailored to those initial conditions and delineates a strategic approach that national authorities may consider when designing their own strategy for modernizing DPS.

The approach covers all relevant aspects of payment systems and instruments that support the provision of DPS. These range from mobile wallets to electronic payments, domestic and international remittances, and real-time (or "fast" or "instant") retail payments. DPS offer affordable and convenient ways for people to make and receive payments and fund transfers and to store value without needing to protect cash as a physical asset. DPS make data analytics available on users' financial lives and enable more efficient assessment of consumers and merchants' creditworthiness. As well, DPS may facilitate assistance in times of need, as people can reach out to their social networks to obtain additional funds from relatives, friends, or donors and for governments to direct benefit transfers. Importantly, DPS can support both women's empowerment

by enabling women to have direct agency over their financial lives and the inclusion of individuals who are financially underserved or excluded from formal finance. Higher penetration of DPS also makes "pay as you go" business models feasible for the delivery of other essential services, such as water and electricity, and thereby has a linkage with various UN sustainable development goals.

DPS, however, also involve risks. Greater connectivity from digital solutions expands the number of entry points for cyber hackers in search of a weak link in the network, complicating the protection of customer data. Incidents might not necessarily result in fraudulent usage of an account; they can extend to compromising personally identifiable information, leading to loss of privacy and other financial and non-financial crimes. Failures to control these risks can lead to rejection in the market and dampen customer appetite for DPS. A critical issue inherent in DPS technologies concerns competition: large technology and telecom firms that enter into financial services may gain significant market shares (particularly in the payments space) and could be a source of increased competition for incumbent financial institutions. While greater competition and diversity in payment services can contribute to a more efficient and resilient financial system, they could result in an uneven playing field for regulated incumbents and further result in a market that is not more competitive but more concentrated, albeit with a shift from incumbents to a few new entrants. Another important concern is financial market integrity, as DPS raise new risks regarding efforts to counter money laundering and the financing of terrorism. Lastly, the development of DPS, if done incorrectly, may carry its own "risk of exclusion," due to lack of trust, inadequate financial and digital literacy, or tight know-your-customer regulations.

NEED FOR STRATEGIC DIRECTION AND POLICY ACTION

Developing sound and dynamic DPS ecosystems requires harnessing market forces to address both supply-side and demand-side barriers while mitigating the related risks. Historically and for a long time, payment services have lain at the heart of commercial banking. In recent years, technological developments have created opportunities for non-bank players to provide new payment-service solutions, including digital payments. However, in many jurisdictions, these new players (for example, telecom network operators) were permitted to operate only through banks (in the context of so-called bank-led models). The strong push from both the supply and demand for innovation from the markets and societies has forced several countries to adopt the regulatory construct of prepaid accounts denominated in the fiat currency and delinked from traditional bank accounts—referred to as electronic money (e-money). Further, countries have allowed non-bank players to issue e-money directly and become payment service providers (PSPs) in competition with banks, and new laws and regulations have been enacted to govern the issuance and handling of e-money. In many MENA countries, there have long been legal and regulatory obstacles for non-bank e-money issuers to operate and for incumbents to use different business models, such as agent banking. Until recently, non-banks had been allowed to issue e-money independently in only two MENA countries: Iraq and Jordan. In the last one or two years—many of them, in fact, in the last few months—several MENA countries and economies have adopted regulatory changes to

allow non-banks to issue e-money independently: Lebanon, Morocco, the West Bank and Gaza, Yemen, Oman, the United Arab Emirates (UAE), Bahrain, and Saudi Arabia.

The MENA region is very diverse, and its countries vary considerably in terms of economic and financial-sector development. The region shows signs of a "middle-income trap"—the term used in the economic development literature to describe the risk of a growth ceiling for middle-income countries—and one of the factors explaining the trap is the MENA region's slow adoption of general-purpose technologies due to barriers that prevent such adoption in key sectors of the region's economies. Digitalization in the region is low, and important gaps remain in the area of DPS, both in terms of infrastructure development and access to services. There are four waves of retail payment innovations: (i) digital access to bank accounts, (ii) delinking of payments from bank accounts, (iii) delinking of payment initiation from account maintenance, and (iv) delinking of accounts from payments. Only Bahrain is currently riding the third wave, while most of the other countries are still between the first and the second. While all MENA countries in the high-income range show advanced DPS features, not all upper-middle-income economies in the region have evolved their DPS in line with their level of economic development (Algeria, Iraq, and Libya are a point in case); on the other hand, lower-middle-income Morocco shows a quite dynamically evolving ecosystem. Also, whereas progress is clearly observable in the region as one moves from bottom up across the different evolution levels of its national DPS ecosystems, progress overall is still modest relative to other regions in the world.

These findings point to two important conclusions. First, each country of the region needs to define its own strategy for further modernizing its DPS ecosystem, based on its own gaps and the demands of its economy. The "multilevel" strategic approach developed in this report builds on a set of general policy actions that fit all MENA countries and designs policy actions that are specific to each level of DPS ecosystem evolution. Second, working only on the supply side (say, by easing regulations) might not be enough to accelerate DPS development. It is essential that national strategies aim also at the demand side of DPS provision, through measures intended to increase the capability of consumers to access and use DPS and their comfort doing so.

A REGIONAL STRATEGIC APPROACH

A regional strategy for developing sound and dynamic DPS ecosystems in the MENA region should ultimately enable each country's ecosystem to

Deliver safe and convenient payment services using state-of-the-art (digital) technologies that enable residents to make and receive fund transfers anywhere, to and from any party, at any time, seamlessly and efficiently, including, importantly, under crisis situations.

The strategic approach to achieve these objectives consists of a set of policy choices articulated in "building blocks" and "drivers" framed together in a consistent framework. The building blocks are the components of a sound and dynamic DPS ecosystem,

while the drivers comprise the actions that the policy authorities and relevant stakeholders should take in order to set the building blocks in place and make sure they all fit together and serve their purpose effectively. Given the high degree of regional diversity, the approach takes into account the different country circumstances and specificities and is "multilevel," where each level refers to one of the following three types of DPS ecosystems:

- **BASIC:** Characterized by a relatively undeveloped DPS ecosystem dominated by banks (where most banks offer only basic payment services with minimal attention to Internet banking, mobile banking, and low-income segments), with no or only few non-bank PSPs mostly acting through banks (typically, mobile-money providers).
- **EVOLVING:** Characterized by the presence of banks that are active in the payments market, or the gaps that banks leave are being filled by non-bank PSPs and some more advanced DPS.
- **INNOVATING:** Characterized by sophisticated services provided by a diversified range of PSPs.

The strategy focuses on the first three waves of innovation referred to above.[1] Its success requires as preconditions the existence in each country of solid payment-system foundations, such as a well-founded, clear, transparent, and enforceable legal basis for all material aspects of the system, and safe and efficient infrastructures for the execution, clearance, and settlement of transactions.

Building Blocks

The building blocks of the strategic approach consist of a number of strategic actions to support the change of DPS ecosystems. These actions are consistent with the payment aspects of financial inclusion (PAFI) framework (CPMI-World Bank Group 2016, 2020) and the Bali Fintech Agenda (IMF 2018) and include (i) open-minded regulation, (ii) safe and efficient infrastructures, (iii) integrity and security, (iv) robust competition, and (v) well-protected, informed, and financially educated customers.

Regulating with an open mind. Legal and regulatory frameworks should be predictable, risk based, and fair. They should allow for new entrants, they should be technology neutral, and they should not impose excessive compliance costs on regulated entities. Stringent prudential regulations should ensure that PSPs are sound and resilient to shocks, and regulations should be "proportional" (that is, requirements should be based on the PSP risk profile) and "functional" (different entities providing the same type of service should be subject to the same set of rules). Also, regulation should encourage PSPs to compete on service provision and to cooperate on issues of common concern and interest (for example, building infrastructures, policy design, interoperability, adoption of standards).

From basic to evolving:

- *Regulators should provide legal backing for digital channels to transact and access bank accounts.*
- *Regulators should permit and enable market entry of non-bank e-money issuers.*
- *Agent-based models should be allowed for bank accounts and e-money issuers.*
- *Regulations should protect the funds that back customers' e-money holdings.*
- *The authorities should have the capacity to balance risk and innovation.*
- *All legal and regulatory aspects relating to payment systems and services should be addressed in a comprehensive and holistic manner.*

From evolving to innovating:

- *New risks (both idiosyncratic and systemic) should be identified and addressed effectively and in a timely fashion.*
- *New tools should be used to streamline compliance requirements for regulated entities and redesign the way regulators collect and monitor the data.*
- *The intervention of sectoral regulators should not obstruct, but promote innovation while protecting the system, consumers, and investors, taking into account in particular the risks associated with financial activities.*
- *Regulation should facilitate "open banking" practices (allowing DPS providers to access their clients' account information, upon client consent, via dedicated interfaces) and facilitate the use of big data while protecting the DPS ecosystem from abuse.*

Setting up safe and efficient infrastructures. Safe and efficient infrastructures are needed to enable effective delivery of DPS. Infrastructures consist of the multilateral systems (including also their operators and participants) that allow for the secure and cost-effective execution, clearing, settling, and recording of transactions. National authorities committed to developing DPS should take a strategic approach to the payment infrastructures that are needed to support DPS delivery and should work closely with the private sector to this end. While, in the short term, the authorities might not insist on interoperability in basic DPS ecosystems (where existing infrastructures do not support it), it is a "must" for those ecosystems that are already at the evolving or innovating level.

From basic to evolving:

- *Efficient and effective infrastructures are needed to facilitate DPS provision.*
- *The authorities should ensure that infrastructures are accessible.*
- *Access criteria should be clear, objective, proportional, non-discriminatory, and disclosed publicly; they should allow for new participants (banks and non-banks) to join.*

- *Access criteria should ensure a level playing field among market participants.*
- *Regulators should, in principle, promote and foster interoperability of systems.*
- *The safety, efficiency, and reliability of the national payment system (NPS) should be enhanced, including through implementation of infrastructures addressing large-value payment systems and securities markets.*

From evolving to innovating:

- The authorities should require interoperability.
- As interoperability is multilayered (for example, across transactions and across systems), the authorities should calibrate its scope on market needs and infrastructure development.
- The authorities should determine whether to facilitate voluntary private-sector interoperability agreements or to impose interoperability requirements.
- The delivery of fast payment services should be facilitated.

Strengthening integrity and security. Payment systems are exposed to risks of integrity and security from criminal activities (for example, fraud, financing of terrorism, money laundering, and information abuse) that emanate from individuals exploiting the weaknesses of the systems (for example, the anonymity of payments, the difficulty of tracking them, the speed with which transactions occur, and the difficulty of monitoring the systems). Regulation should require licensed systems and PSPs to manage such weaknesses through a combination of measures, such as customer due diligence requirements, security requirements and consumer protection in digital payments, high transparency and consumer information on security standards, and limits on deposit or transfer amounts.

From basic to evolving:

- *Customer due diligence rules should be progressive or tiered.*
- *Systems should be able to identify customers and record transactions digitally.*
- *Systems and services should be protected from cyber risk and the risk of fraud.*

From evolving to innovating:

- Higher security and integrity-protection modalities should be implemented for more sophisticated DPS ecosystems.
- Centralized solutions should be considered for managing fraud risk.

Strengthening competition. Competition is necessary for developing sound and dynamic DPS ecosystems. Competition policies should reflect the level of DPS ecosystem development. While policies for basic ecosystems should focus on market-entry issues, market conduct and market structure become central for the higher levels and for accompanying the evolving-to-innovating transition.

From basic to evolving:

- *The authorities should facilitate competition by opening the DPS market to new entrants.*
- *The authorities should protect the DPS market from anticompetitive practices and ensure that PSPs conduct their business in line with competition principles.*

From evolving to innovating:

- *In addition to the above policies, in more sophisticated DPS markets, competition policies should guard against the anticompetitive behavior of large multiproduct service providers and, in general, all entities holding significant market power through a combination of ex ante regulation and ex post enforcement.*
- *The authorities should prevent or penalize excessive and discriminatory pricing practices.*
- *The law should clearly define which authority (authorities) are responsible for DPS competition issues and grant to it (them) sufficient powers and autonomy, including to enforce rules and decisions. Enforcement of competition rules in DPS provision can be attributed solely to the competition agency or jointly with the central bank and the telecommunications regulator.*
- *In jurisdictions where a competition authority coexists with sector regulators that share competition responsibilities, all agencies should coordinate their acts. Where there is no established competition authority, sector-specific regulators should be empowered and encouraged to lead and define a coordinated way forward on competition issues and to streamline enforcement.*
- *The competition authority should be resourced with specific expertise and collaborate with the payment-system regulator.*

Protecting, informing, and educating the consumer. A sound and dynamic DPS ecosystem requires consumer confidence, which, in turn, requires that consumers perceive the DPS ecosystem both to be reliable and to provide them with sufficient protection of their rights as customers. Regulators should ensure that the relevant networks, platforms, and other technical elements for DPS delivery are in place and function properly. They should also require PSPs to adopt quality-of-service standards and risk-management practices that are appropriate to the nature of the DPS delivered, and they should monitor the PSPs' performance and compliance with rules on an ongoing basis. Finally, regulators should establish PSP liability rules for losses suffered by consumers caused by such events as fraud, agent misconduct, or quality-of-service issues (for example, network downtime).

From basic to evolving:

- *Clear rules for transaction disputes should be instituted for all payment methods, as well as for transparency and customer information.*
- *The funds backing customers' e-money holdings should be protected.*

- From evolving to innovating:
- *Customer data should be protected.*
- *DPS literacy and awareness should be enhanced.*

Drivers

The drivers of the strategic approach consist of actions that the public authorities and relevant stakeholders should undertake in order to set in motion the development of a sound and dynamic DPS ecosystem. They ensure that the appropriate building blocks of the strategy are in place and work together effectively. Drivers include (a) overseeing the DPS ecosystem effectively; (b) inducing cooperation between the DPS overseer and other relevant public authorities; (c) engaging stakeholders in the policy dialogue on DPS issues; and (d) acting strategically and with discipline. The drivers for a specific level of DPS ecosystem are (e) leveraging large-volume, recurrent payment streams and (f) broadening merchant acceptance of DPS.

Ensuring effective oversight. Strong oversight is key for building sound and dynamic DPS ecosystems. Oversight seeks to ensure that DPS provision is safe, efficient, and inclusive; robust and resilient to risks; constantly available; and evolving based on the changing needs of the economy. The overseer should be given enough authority and resources to conduct effective oversight and to use all instruments necessary to this end, and the overseer should use its authority and authoritativeness to balance cooperation and competition in the market for DPS. The overseer of the DPS ecosystem may play several roles: it adopts rules, standards, and policy guidelines for the good conduct of PSPs, and it monitors and ensures PSP compliance with such rules, standards, and guidelines. It acts as regulator and supervisor of DPS provision, and it makes sure that PSPs, as well as all entities operating in the NPS, carefully manage the risks that arise from their payment activity and that such risk do not become systemic. The overseer should also encourage cooperation from NPS stakeholders and coordinate their action when this is necessary to increase the efficiency and safety of payment infrastructures. An important part of the oversight role is to catalyze the modernization of the NPS; in that context, the overseer promotes use of DPS and the protection of DPS user rights. The adoption of risk-based rules and oversight tools and the capacity to hold an ongoing policy dialogue with stakeholders are necessary ingredients for the overseer to strike a sound balance between these two objectives.

Taking a cooperative approach. Developing a sound and dynamic DPS ecosystem entails cooperation at multiple levels, between the DPS overseer and other relevant authorities and between the overseer and DPS stakeholders. Such cooperation needs to be effective in normal circumstances and should be adequately flexible to facilitate effective communication, consultation, or coordination, as appropriate, during periods of market stress, crisis situations, and the potential recovery, wind-down, or resolution of PSPs. Cooperation may also be important at the regional and international level. The overseer should be committed to advancing DPS initiatives through leadership and action.

Acting strategically and with discipline. The authorities should ensure that all related and concurrent strategies (for example, payment-system modernization, transition to e-government, and financial inclusion) be mutually consistent and coordinated. Successful transition to a sound and dynamic DPS ecosystem requires strategic and disciplined action. The DPS overseer should adopt an operational strategy for developing the national DPS ecosystem that combines the "building blocks" and organizes the "drivers" referred to above. The overseer, in cooperation with the stakeholders, should then implement the strategy and monitor its implementation systematically, taking corrective action if necessary. Acting strategically requires careful stocktaking at the outset of the strategy process and close monitoring during strategy implementation.

- *Stocktaking, possibly supported by benchmarking, is necessary for strategy preparation, as the policy makers and stakeholders need to have a clear picture of the DPS ecosystem as it stands before taking action.* A comprehensive stocktaking should reflect a full description of the existing structure of the ecosystem and incorporate a gap analysis that identifies the missing components, the vulnerabilities that the strategy should address through appropriate policy actions, and the impediments to DPS development that need to be removed. Benchmarking the ecosystem against select (qualitative and quantitative) indicators would help to show how the ecosystem compares internationally and what could realistically be achieved through the strategy to modernize or reform it.
- *Monitoring strategy implementation is essential to assess progress.* It requires the use of a comprehensive and robust national data-measurement and evaluation system and should build upon the information and indicators used for stocktaking and benchmarking, with a view to assessing the impact of strategy implementation against the goals set, identify obstacles to implementation, and provide insights about the efficiency, effectiveness, and impact of the reforms and policy programs deployed. Tracking progress could be supported by establishing an online data portal and by publishing regular reports to provide publicly available data on the adoption and use of DPS. The World Bank has elaborated templates for stocktaking and for assessing progress on the use of digital financial (and payment) services. The national authorities implementing the strategic approach developed in this report could adopt the templates as tools (World Bank Group 2018a, 2018b).

ADDRESSING THE MENA REGION'S CRITICALITIES

Sound and dynamic DPS ecosystems would assist MENA countries in their efforts to increase their people's access to finance. Reducing the cost of using DPS, increasing its convenience, simplifying the requirements for using DPS, and, most of all, strengthening public trust in the DPS ecosystem (including also its institutions and instruments) would go a long way toward addressing the factors that people in the MENA region consider as major obstacles to access finance: gender discrimination, limited competition in the banking sector, and youth unemployment. Specifically:

On gender issues, governments in the region should make the gender divide in DPS a priority. Customer due diligence policies should be proportionate and risk based, and a strong commitment to customer protection would boost women's trust of DPS providers.

On competition in banking and finance, new payment and financial digital technologies may open up the financial sector in the MENA region to new providers, thus creating a new competitive environment. Within this new environment, banks and other new players may become competitors within individual elements of the value chain and work together in other areas.

On access to payment services for youth, along with the gender divide in access to payment services, the divide between youth and other adults is significant and needs attention from public authorities. Digital payment and financial services can help youth in the MENA region to access resources to build their job skills and manage income sources. DPS and digital financial services can help families manage major expenses linked to educational and training opportunities, and digital platforms can open unprecedented opportunities for youth to access education, training, goods, markets, and financial and non-financial services. DPS can also help youth access and participate in the digital economy.

Finally, on narrowing the informal economy, the digitalization of payment services offers a very important way to create demand for access to regulated financial services, starting with access to payment services. However, in order to fulfill its potential, digitalization also requires attention to financial consumer protection, financial education, and simplifying and incentivizing formalization.

DPS FOR GOVERNMENT-TO-PERSON PAYMENTS IN NORMAL TIMES AND EMERGENCIES

DPS are a key enabler for the broader shift of government social-protection programs to direct transfers in both normal times and emergency situations, such as the ongoing COVID-19 crisis. Over the last several years, government social-protection programs have shifted from in-kind and subsidized goods and services to direct transfers of funds. DPS are a key enabler of this trend. These payments, along with other payments from governments to individuals—say, a civil servant's salary—are collectively referred to as government-to-person payments. The shift to DPS engenders efficiency gains for the public authorities, improves the overall integrity of the government-to-person payments, and, when done right, can expand financial inclusion and catalyze development of the DPS ecosystem. COVID-19 has given further impetus to this, given the restrictions on physical contacts, which make the role of DPS even more crucial. The approach recommends measures for extending the use, availability, and continuity of DPS for the residents of crisis-hit countries so they can access essential services and make/receive payments. Important measures include the quick deployment of DPS solutions tailored to vulnerable and financially excluded populations, the dissemination of awareness and

assurance of financial consumer protection, measures for payment systems and other financial market infrastructures, and measures for the continued provision of critical payment services.

This report is intended to benefit primarily central banks and governments throughout the MENA region. The report is addressed as well to relevant national authorities, such as telecoms regulators and competition agencies, which have a critical role to play in DPS ecosystems. Potentially, the effects of the report will also spill over to other nations that have embarked on the process to digitalize payment services and will be useful for NPS stakeholders, helping them take a comprehensive view of the payment ecosystem in which they operate and their role in its development. The report would also support the staff of the World Bank and other multilateral agencies as they assist initiatives to reform the financial sector in the region.

1

INTRODUCTION

This report has been prepared to inform the ongoing MENA Tech program and is directly linked to the cashless payments Marrakesh 2021 targets. The objective of the MENA Tech program is to help World Bank Group teams and external stakeholders achieve regional priorities for digital transformation of government and the economy and regional integration, with a particular and initial focus on reaching the Marrakesh targets for connectivity and cashless payments. MENA Tech aims to achieve this by providing analytical tools, including frameworks, data, analytics, and knowledge-exchange opportunities to operational teams, clients, and regional stakeholders. Further, this paper will serve as a background document, along with other reports (Gévaudan and Lederman 2020), in the preparation of an upcoming flagship report emphasizing the importance of the overall digital agenda for the Middle East and North Africa (MENA) region.

This report discusses strengthening the provision of payment services in the countries of the MENA region as an essential step to integrate their economies into the world of "digital finance and digital economy." Driven largely by the private sector, digital technology as applied to finance is changing the way finance is done today and is likely to alter permanently the landscape of the financial industry globally. The concept of "digital" refers to the technologies and capabilities (such as networks and connectivity, computing, and information storage) that enable the digitization of back-end processes as well as the interaction between users of digital services.[2] The concept of "digital financial services" (DFS) refers to all types of financial activities executed and delivered over the Internet or mobile or other electronic public networks, and whose supply is essentially automated or involves only minimal human intervention. It encompasses all aspects that are affected by digital technologies, from process and products to delivery channels of financial services (for example, via mobile devices). It includes a vast range of financial and non-financial entities that operate throughout the distribution chain of financial products (from wholesale to retail) and populate the relationships between financial institutions and between them and their customers (figure 1). The key entities operating in the DFS space, in addition to the incumbent financial institutions, are the fintech companies ("fintechs")—that is, those firms that adopt technology-

enabled innovations in financial services that could result in new business models, applications, processes, or products with an associated material effect on the provision of financial services (FSB 2017).

Digital finance has significantly changed the way people do finance every day and has enabled the digital economy. In many countries around the world, people have the ability to check balances on a real-time basis, transfer and receive money electronically, and pay bills online. They can assess on-screen economic information that is relevant to their activity, and they can buy and sell securities basically from every location where they can use a digital device. Also, in Asia and much of Africa, insurance companies have embraced the data and payment infrastructure provided by mobile telephony, revolutionizing the provision of insurance to first-time buyers, and improved customer experience in areas like claims processing (Wrede 2018). The Internet makes available investment strategies and real-time stock quotes and enables powerful and sophis-

FIGURE 1: Fintech Is Transforming the Financial Industry

EVOLUTION OF FINANCIAL SERVICES[1]

User needs	Traditional model	Gap[2]	Technical Innovations[3]				Fintech solutions
			AI/ML	Data cloud platforms	DLT/ Crypto	Mobile	
Pay	Cash/ATM Check Wire/MOT's Debit/ Credit cards Centralized settlement	Speed Cost Transparency Access Security	L	H	H	H	Virtual currencies Remittances Mobile payments Mobile PoS P2P payments B2B transactions DLT-based settlement
Save	Bank deposits Mutual funds Bonds Equities		L	H	H	L	Virtual currencies Mobile market funds Blockchain bonds
Borrow	Bank loan Bonds Mortgages Trade credit		H	H	H	L	Credit modeling Platform lending Crowd-funding Blockchain bonds Auto-underwriting
Manage risks	Brokerage underwriting Structured products Trading regulatory Compliance KYC Insurance		H	L	H	L	Regtech, Smart contracts Suptech Crypto-asset exchanges eKYC, Digital ID
Get advice	Financial planner Investment advisor		H	M	L	M	Robo-advising Automated wealth management

Source: : IMF-World Bank (2019).

1 This figure maps users' needs for financial services—explained in IMF (2017a){-SOURCE NOT IN REFERENCES-}—to traditional and emerging fintech solutions. In doing so, it flags the key gaps that technology seeks to fill and which new technologies are applied in different services.

2 In gaps, transparency encompasses search and matching frictions, while access encompasses product tailoring needs.

3 "AI/ML" refers to artificial intelligence and machine learning algorithms applied to extract insights from large amounts of data. "Data/Cloud Platforms" are cloud-based technologies that facilitate business-to-business, consumer-to-business, customer-to-customer, and business-to-consumer exchanges of data via application programming interfaces across fintech firms, financial institutions, customers, and governments. Access to digital platforms can be secured with digital identification technologies, such as biometrics. "DLT/Crypto" captures distributed ledgers, such as smart contracts and related decentralized technologies. "Mobile" refers to feature phones and smartphones running financial apps. The color scheme reflects a judgment on whether the specific technology has a low (L), medium (M), or high (H) level of benefit for the corresponding fintech solutions. Scaling is purely illustrative.

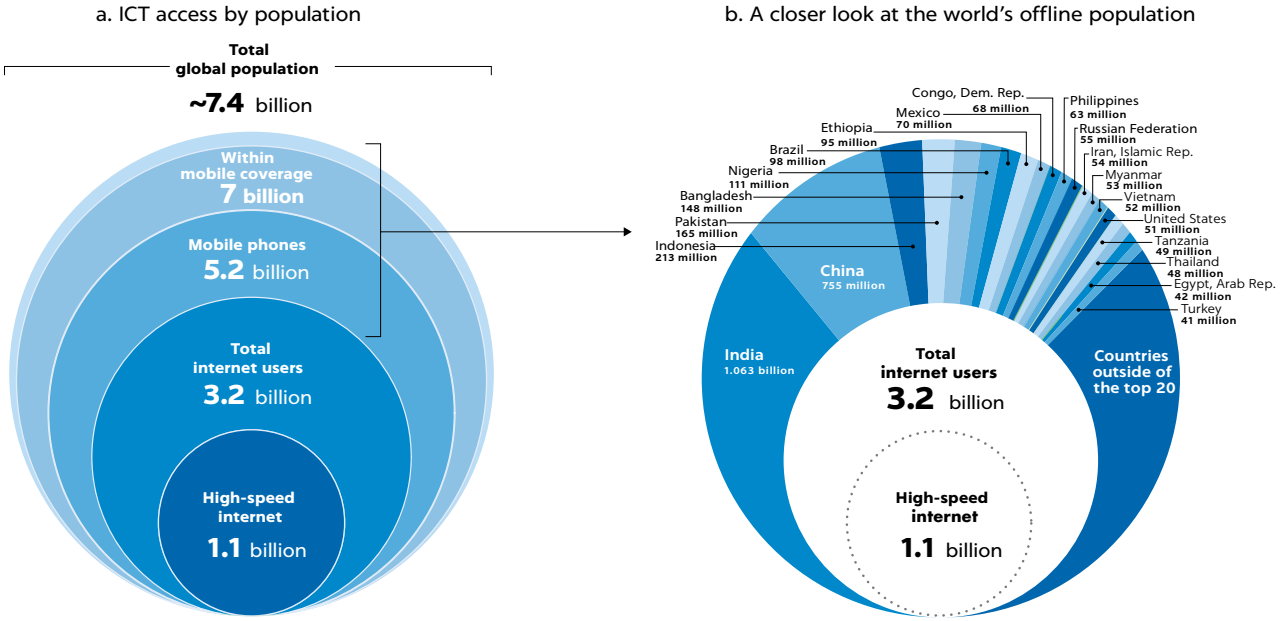
ticated online resources for trading and portfolio management. Before the Internet, financial education was derived largely from books, television, and face-to-face meetings; with the Internet, an unprecedented wealth of information is available to everyone at the click of a mouse. Today, millions of websites and blogs are dedicated to illustrating how the masses can take control of their finances.

The digitalization of commerce has meant that customers expect more convenient experiences across the services they use. The ability of Internet-connected devices to complete transactions in real time has given rise to higher customer expectations with regard to convenience, speed, cost, and user-friendliness of financial services, and consumer comfort with online financial transactions has grown as online business innovations have deepened this rising acceptance of new technologies. *Digital finance makes markets work better by improving access to information and communications, and it pushes toward more competition in the market. It* creates *opportunities and challenges for consumers, financial and non-financial firms, service providers, and regulators and involves risks that need to be identified and mitigated.*

This report deals especially with digital payment services (DPS) and with providers of such services (including also fintechs specialized or involved in their provision).[3] Digital (or electronic) payments are transfers of value that are executed and/or received using digital (or electronic) devices and channels to transmit the instructions. They include payments that are initiated by mobile phone or computer. Card payments are considered to be digital payments. Notice that while the terms *digital* and *electronic* can be used interchangeably to mean the same thing, the report will use the word *digital* in reference to payments. DPS have enabled business models extending beyond traditional e-commerce to the sharing economy (ride share, home share, and so on), the *gig* economy, and the small payments that underpin the app economy; they are also central to new decentralized business models enabled by blockchains and the IoT (Internet of Things).[4]

More broadly, the application of technology to finance is helping the world to become more prosperous and inclusive. Digital technologies have boosted growth, expanded opportunities, and improved service delivery, and digital finance has spurred financial innovation, raised economic efficiency, and is promoting financial inclusion (World Bank Group 2016).[5] Yet the capacity to seize these formidable opportunities remains unequally distributed both within and across countries As great progress is being observed in most countries around the world, many people are still left out because they do not have access to digital financial technologies, starting from the recognition that the Internet remains unavailable, inaccessible, or unaffordable to a majority of the world's population (figure 2). Defining strategic agendas and investing resources to develop digital finance and to connect citizens digitally within the financial space and beyond have taken strategic priority within the policy programs of national governments worldwide. This is happening in the MENA region as well, although countries in the region vary widely in terms of both where they stand with respect to digital financial development and the speed at which they are proceeding toward financial digitaliza-

FIGURE 2: The Internet Remains Unavailable to a Majority of the World's Population



Source: World Bank Group (2016).

tion. As per World Bank classification, the MENA region comprises the following countries and economies: Algeria, Bahrain, Djibouti, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Malta, Morocco, Qatar, Saudi Arabia, Syria, Tunisia, the UAE, the West Bank and Gaza, and Yemen.

The World Bank Group is assisting its client countries in the MENA region in their effort to digitalize finance. Essential to this end is the ability of the people in the region's economies to transfer values electronically—that is, their ability to use DPS. This is premised on the consideration that the availability of efficient, accessible, and safe DPS is a prerequisite for granting people access to digital finance. More broadly, DPS are indispensable to the functioning of digital economy, which rests on the economy's ability to transfer funds with finality,[6] securely, and in real time, either on request by customers or whenever payments are due pending existing obligations. Special policy attention must therefore be placed on making sure that national (or regional) strategies for financial digitalization are supported by adequate infrastructures for the provision of safe and efficient DPS.

This report elaborates a strategic approach for developing sound and dynamic DPS ecosystems as foundations for effective financial digitalization and the development of the digital economy in MENA countries, and covers all relevant aspects of payment systems and instruments that support the provision of DPS to end users. The report builds upon the well-established relationship between financial-sector development and economic and social progress.[7] By building a strong financial sector and developing modern financial services, countries in the MENA region can escape the middle-income trap and expand their social and economic-inclusion programs.

The report is not about intervening in the MENA region through a coordinated regional strategic plan. Rather, it describes what MENA countries should do in order to modernize their DPS ecosystem, starting from their own initial conditions. To this purpose, the report identifies steps that are tailored to those initial conditions and delineates a strategic approach that national authorities may consider when designing their own strategy for modernizing DPS.

The report is organized as follows. Section II discusses the ongoing revolution in the area of payments, including recent innovations, their benefits, and their associated risks; the section also highlights the importance of an appropriate regulatory architecture to support sound and dynamic DPS ecosystems. Section III evaluates progress in the usage of DPS observed in the MENA region and contrasts it with progress observed internationally; the section looks at country statistics to assess how differently national DPS ecosystems have evolved across the region and identifies opportunities and challenges of DPS development in the MENA region. Finally, section IV elaborates a multilevel strategic approach for developing sound and dynamic DPS ecosystems, taking into consideration their different levels of evolution in the region's countries.

AUDIENCE

This report is intended to benefit primarily central banks and governments throughout the MENA region. The report offers them the elements needed to form a coherent vision and strategy for developing the DPS ecosystems of their countries, taking due account of local initial conditions and challenges. The report is also addressed to relevant national authorities, such as telecoms regulators and competition agencies, which have a critical role to play in the context of DPS ecosystems. Potentially, the report's effects will spill over to other nations that have embarked on the process to digitalize payment services. In addition, it is hoped that the report will be useful for NPS stakeholders, helping them in particular to appreciate the importance of taking a comprehensive view of the payments ecosystem in which they operate and their role in its development. Finally, the report would support the staff of the World Bank and other multilateral agencies as they assist initiatives to reform the financial sector in the region.

2

INNOVATION IN THE BUSINESS OF PAYMENTS

A RAPIDLY CHANGING BUSINESS ENVIRONMENT

Innovation in the area of retail payments is relentless, ranging from introducing new products (including new media of exchange) to building new transaction channels and changing the infrastructure to make payments faster and peer to peer. DPS span a broad range of services. These include, among other things, mobile wallets,[8] electronic payments (between people and enterprises and to/from government), foreign-exchange transactions, domestic and international remittances, and real-time (or *"fast" or "instant"*) payments.[9] Accessible and deliverable through digital channels, DPS offer affordable and convenient ways for individuals, households, businesses, and governments to make and receive payments and fund transfers. They allow people to store value without needing to protect cash as a physical asset, to access faster fund-transfer facilities, to make and receive payments, to borrow, save, insure, and invest, and to manage a person's or enterprise's finances. DPS make data analytics available on users' financial lives and may thus increase their willingness to save. Similarly, by allowing individuals' transaction histories to be recorded and analyzed, DPS enable more efficient assessment of the creditworthiness of consumers and merchants.

DPS can also reduce the costs and increase the coverage of remittances. They make transfers of small amounts viable and allow people (especially those living in remote places) to receive part of their annual income or benefits through domestic and international money transfers. DPS enable remitters to direct funds directly to savings, health, education fees, or other types of targeted accounts, thus ensuring that funds are spent as intended. DPS may also facilitate assistance in times of need, as people can reach out to their social networks to obtain additional funds from relatives, friends, or donors. Importantly, DPS can support women's empowerment in that the digital nature of financial remittances permits recipients to keep financial transactions private, even within their households.[10]

BOX 1 INNOVATIONS IN PAYMENTS: A STYLIZED ILLUSTRATION

In a highly stylized fashion, the following four waves of innovation can be distinguished in the retail payments business, starting from

i) ***The digitization of bank accounts,*** allowing account holders to mobilize and to access their funds electronically through Internet banking in the 1990s to mobile banking at the turn of the century; to

ii) ***The delinking of payments from bank accounts*** through the introduction of the prepaid concept, whereby value can be stored in special-purpose accounts (prepaid accounts) and accessed and transacted through digital devices and channels, which led to the creation of mobile money; to

iii) ***The delinking of the initiation of payments from the maintenance of accounts***, so that third-party PSPs may provide payment-initiation services to customers holding accounts with other financial institutions through such initiatives as open banking via application programming interfaces (APIs)[11] and tokenization;[12] and finally to

iv) ***The delinking of accounts altogether from payments,*** which allows agents to effect electronic fund transfers without having to hold an account with a financial institution—this is the world of distributed ledger technology, crypto-assets, cryptocurrencies, and stablecoins.[13]

These four waves have been accompanied by deep changes in the processing of payments and service delivery, aimed at offering users increasing levels of convenience in terms of speed (for example, faster payments), ease of access (for example, different transaction channels), and ubiquity (for example, QR codes). New business models have also developed that today allow payments to be integrated into the day-to-day interactions of users, rendering them "invisible" and "contextual" (see box 15), and allow for the accumulation of big data, which can be used to analyze users' behaviors and preferences and thereby to identify better ways to match their demands.[14]

Four waves of innovations can be distinguished in the retail payments business: from those that (i) facilitate the mobilization of bank deposits through digital access to bank accounts to those that (ii) delink payments from bank accounts, (iii) delink the initiation of payments from the maintenance of accounts, and (iv) delink accounts altogether from payments. Box 1 and appendices A and B illustrate the evolution of the payments business and regulation, and box 2 describes the benefits accruing to DPS stakeholders. Only Bahrain is currently in the third wave of payments innovation, while most other MENA countries are somewhere between the second and the third wave. The fourth wave is still unfolding, and it is not yet clear whether it affords any substantial advantages in terms of advancing financial inclusion. More importantly, its broader risk implications for financial stability and integrity raise concerns. Hence, in this report, the fourth wave is addressed only from the perspective of preparing the necessary legal frameworks and monitoring developments, while no efforts to embrace it is advocated. It should be noted, however, that the underlying technologies of crypto-assets (blockchain and distributed ledger technology) have other applications beyond payments and financial inclusion that lie outside the scope of this strategy.[15]

BOX 2 BENEFITS OF DIGITAL PAYMENT SERVICES

While service providers have tangible costs in running and managing DPS, and merchants (in traditional cases) have costs for accepting them, key stakeholders can reap the following multiple benefits by adopting them:

For Retail Merchants

- Security: Cash is more liable to theft, loss, and fraud
- Better and faster ability to assess the health of their business operations (for example, cash flows, profit and loss) through synergies with e-payments
- The ability to generate revenue from new channels and DFS (if the merchants keep balances with banks and other PSPs
- Access to credit based on either digital payment payables or the ability to show documentary trail of financial well-being based on the digital payments
- Value-added services that come bundled with payments or for making or receiving payments (for example, loyalty, credit, marketing support)

For Customers

- Simpler payment method in cases where customers already manage and receive their finances through a deposit transaction account
- Pay for goods and services on a lay-away or pay-as-you-go basis
- Payment options that closely match customers' ability to pay
- Savings through access to loyalty schemes and promotions
- Extension of purchasing power via access to a revolving line of credit (for products such as credit cards), often interest free if paid in full at the end of the statement cycle
- Enhanced ability to assess spending patterns and manage budgets
- Building a transaction history and other relevant electronic data trails that may give customers easier or faster-processed access to credit

For Suppliers

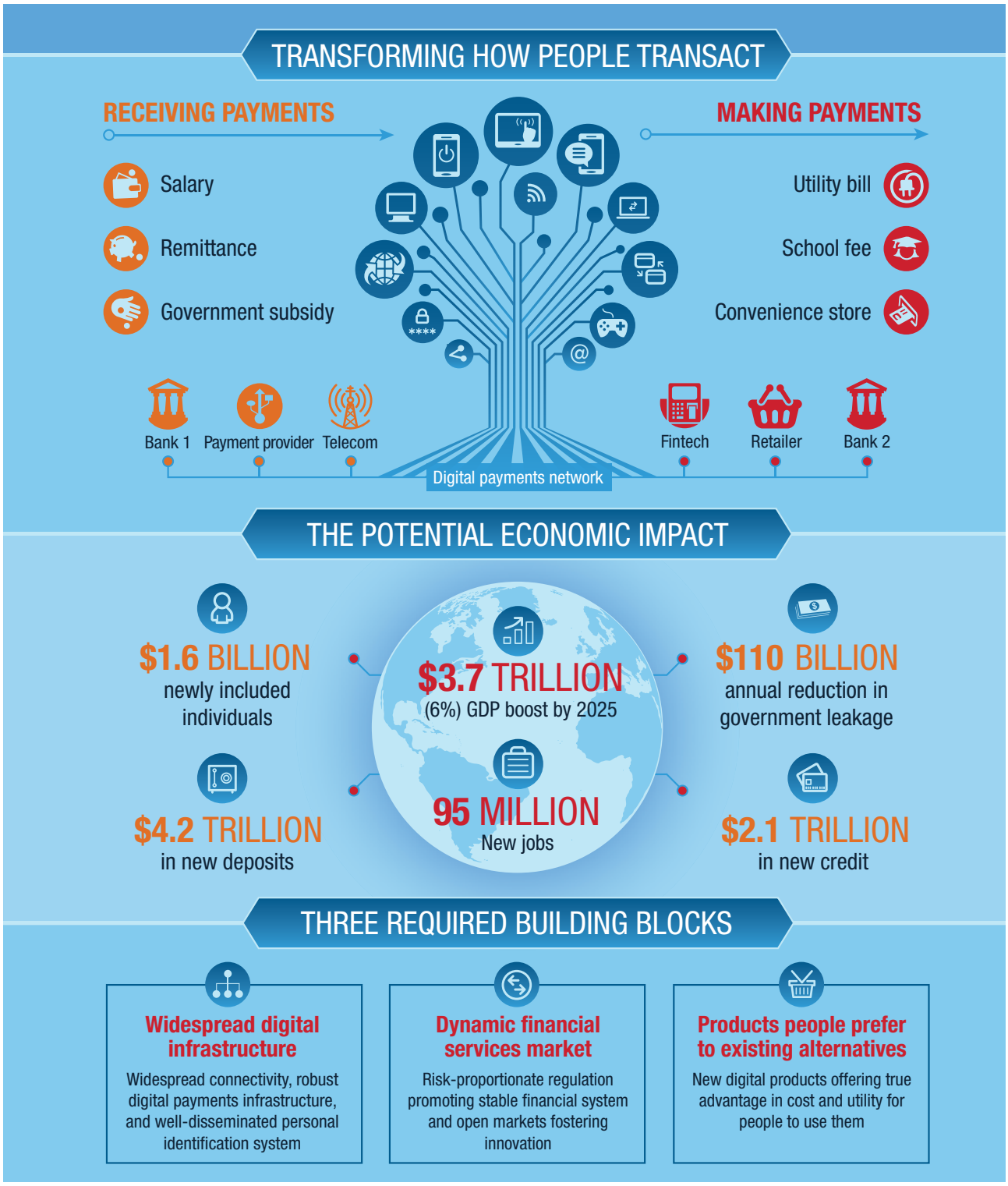
- Lower operational costs and risks from cash collections
- Better ability to provide short-term liquidity to retailers and managers, or to enable a bank to manage credit to retailers better
- Enhanced infrastructure to manage marketing promotions, loyalty schemes, and sales incentives
- Less frequent need for retailers to place large orders
- For PSPs
- Fee income from either payment or adjacent services (financial and non-financial)
- Opportunity for cross-selling
- Enhanced ability to monitor performance with retailers
- Opportunity for collaborators to earn part of the overall revenue or to sell adjacent services

For Governments

- Better tools to monitor trends in consumer spending and the retail sector
- Expansion of financial access and inclusion
- Expansion of the tax base through formalizing enterprises and possible reduction of leakage
- Growing evidence that shifting spending behavior to electronic payments can increase overall economic output and enhance social welfare

Source: Principles (2017).

FIGURE 3: Digital Payment Services and Financial Inclusion



Source: McKinsey Global Institute (2016b).

DPS can greatly benefit large segments of the population, especially the poor, and they can support the inclusion of individuals who are financially underserved or excluded from formal finance (figure 3). Some key attributes can make them especially suitable for financial inclusion, especially as DPS can be attached to transaction accounts held with banks or other authorized and/or regulated payment service providers (PSPs), which can be used to make and receive payments and to store value.[16] These accounts may vary in price and service offerings and range from accounts with a limited set of services and offered at very low or zero fees and no minimum balance requirement to full-fledged retail customer or corporate accounts. They enable customers to conduct transactions remotely (and speedily) and at agent locations instead of bank branches.[17] Prepaid instruments based on e-money transaction accounts are used to provide access for previously financially excluded individuals to their first transaction account and to help individuals to get acquainted with more sophisticated financial products and eventually enhance their ability to participate in the digital economy. In fact, DPS can create a *"pull"* to open transaction accounts, in particular when they get embedded into incoming payment streams such as government-to-person payments, salaries, and wages; non-discretionary spending such as bill payments; and digital economy services that touch day-to-day lives, such as ride sharing. Properly regulated payment services supported by agents are well suited for rural and isolated areas, where providing physical points of access to cash and payment services can be expensive relative to the potential revenue streams. Customers that currently are not served by banks due to the small or zero profit margin associated with their transaction activities might become more attractive at lower cost structures, and a new class of players might be more motivated to cover this market segment.

DPS, however, also involve risks (box 3). Greater connectivity from digital solutions expands the number of entry points for cyber hackers in search of a weak link in the network. This may be particularly relevant for client-facing applications using customer data, and new devices, including those connected to the Internet of Things. Indeed, incidents often involve fraud and theft through mobile banking apps, and breaches of personally identifiable information. Factors that contribute to a new type of fraud is the lack of cues in online interactions and the speed of the transaction, which leave no room for any recourse. Further, criminals use sophisticated social-engineering attacks that create a sense of urgency, combined with information gathered about the customer through illicit means. Hackers convince even diligent customers that it is their own bank or PSP that is interacting with them, and thus trick them into performing transactions under false pretenses. These techniques, combined with faster payment services, which are by design irrevocable, create an ideal situation for criminals.[23] Failures to control these risks can lead to rejection in the market and dampen customer appetite for DPS as a whole.[24]

A critical issue inherent in DPS technologies concerns competition. Large technology and telecom firms that enter into financial services with established networks and accumulated big data may gain significant market shares (particularly in the payments space) and could be a source of increased competition for incumbent financial institutions. While greater competition and diversity in payment services can contribute

BOX 3 RISKS OF DIGITAL PAYMENT SERVICES

In addition to the risks discussed in the text, it may be helpful to consider the results of a recent research by the Bill and Melinda Gates Foundation (2015), which has developed a framework to evaluate the risks associated with the new entities entering the DPS market, their new products, and the rapidly evolving DPS value chain. The research examines whether the increasing role of non-bank providers and the development of innovative distribution channels create new types of risk for consumers, providers, and the financial system at large and concludes that, while DPS do not introduce major new risks beyond those that exist already in traditional payments, they do raise old risks across a much longer value chain populated by many new players, as the range of activities needed to create DPS continuously expands and attracts an increasing number of non-bank providers.

Interestingly, the research found that, in the area of DPS, operational risk is by far the most significant type of risk affecting both providers and customers, and its impact can be analyzed in terms of three types of process breakpoints: technology failure, human error, and malfeasance. The largest type of operational risk to customers (in terms of severity and likelihood) is human error. Such error can cause money to be deposited or sent to the wrong account. The greatest risk to providers is malfeasance and is driven largely by the risk of a hack into a provider's back-end accounts that drains user funds.

While technology failure is today the smallest risk for both providers and consumers, the most important sources of operational risks to both consumers and providers will increasingly originate from technology risk and technology-enabled large-scale fraud (for example, a system hack) as processes become ever more digitized.[18]As an example, take the case of the person-to-person mobile-money remittance process. During the initiation step, the system typically asks the money sender to enter the phone number of the recipient of the transfer and then to select "enter" on a mobile phone menu. Things that might go wrong here include breakpoints of all three types. For instance, the money sender could encounter trouble with the cellular network as the information is transmitted (technology malfunction). The payer could also mistype the recipient's phone number (human error), or the payer could be trying to send money for illicit purposes such as the financing of terrorism or as part of an attempt to launder money (malfeasance). Smart phones or other factors can change the details of potential breakpoints.[19]

Indeed, DPS may also help manage and mitigate important risks. DPS also mean that recipients can choose when to collect their cash payment, which improves security and allows them more discretion over how the money is used. This was cited as a major benefit by program managers and recipients alike in the Haiti earthquake response, where levels of robbery and crime were a significant threat to physical cash distributions at designated locations. Similarly, the government of Pakistan's 2009 flood response delivered one million prepaid smartcards to recipients in 70 days, probably the largest emergency response using DPS. This response could not have been delivered at such speed without the preexisting use of branchless bank agents and a sophisticated national ID system.

A recent report reviews the use DPS in four emergency cash-transfer programs and details considerable benefits, including improved security for staff and recipients, reduced leakage, improved reconciliation and control of expenditure, greater speed and efficiency of transfers, and reduced costs for the agency and recipient.[20] However, the existence of a functioning network of payment agents and enabling regulatory infrastructure was noted as key to these positive outcomes—something that is unlikely to be in place in many emergency contexts, particularly those in low-income countries or fragile states. Where there is no agent network, the relatively short term of emergency-response programs and the smaller recipient base compared to longer-term cash-transfer programs may make DPS unviable in many emergency-response contexts.

BOX 3, continued

DPS have the potential to reduce leakage and corruption.[21] Unique recipient identifiers, such as biometric recognition devices or personal identification numbers (PINs), can reduce payment to the wrong recipient. Paying cash directly to technological devices such as mobile phones that are owned by recipients can also reduce opportunities for bribes. Record keeping for better monitoring of cash payments is stronger, with point-of-sale devices providing electronic and paper records of payments for the recipient and payment provider alike. In Argentina, after the Ministry of Social Development switched from cash payments to a prepaid debit card, the number of participants who said they paid a bribe to access their benefits dropped twelvefold. And in the 2011 Horn of Africa drought response, cash transfers were perceived as less prone to corruption than food assistance, in part due to strong record keeping associated with DPS.[22]

to a more efficient and resilient financial system, heightened competition could also put pressure on financial institutions' profitability, thus leading to additional risk-taking among incumbents in order to maintain margins. In other scenarios, however, the participation of large fintechs may not result in a more competitive market over the longer term, and their greater market shares may be associated with unchanged or higher concentration, albeit with a change in composition away from traditional players.[25] It should be noted that, while competition on services historically led to the eventual development of shared infrastructure (consider Visa and Mastercard, for example, as well as the case of telecom companies that created tower-sharing arrangements as their industry matured), the dynamics have changed in recent years, as some of the new entrants are able to scale so rapidly that they corner a big share of the market and have no incentive to join consortiums or share infrastructure. This dynamic requires public authorities to enhance their monitoring and readiness to step in.

Another important concern relating to the use of DPS is financial market integrity.[26] DPS raise new risks and challenges with regard to anti-money laundering and countering the financing of terrorism (AML/CFT). New areas of vulnerability might develop due to the anonymity of DPS users, decentralized governance of new PSPs without accountability, and ease of cross-border transactions—all factors that make the monitoring of financial market integrity more complex for public authorities. Finally, as new financial players are reshaping the financial sector, they may be outside the scope of current payment regulations and thus subject to less stringent AML/CFT rules than incumbent institutions. If not proportionate to the AML/CFT risks, these regulatory gaps or loopholes may lead to increased potential for financial crime. At the same time, new technologies may support greater efficiency for AML/CFT policy. "RegTech" companies are especially keen to enter this field, which could attract significant investment by PSPs.[27] Analytics of nonstructured data associated with artificial intelligence and machine learning can support PSPs' financial crime functions in the monitoring and reporting of suspicious transactions.[28] While non-face-to-face relationships are usually considered as a high risk for AML/CFT, technologies such as biometrics (for example, fingerprints, vocal recognition, touch iden-

tification) and scanning technologies, as well as new sources of data from daily social and commercial interactions, may help identify fraud in a digital environment and promote remote but secure customer identification and authentication processes. E-identification and e-signatures may provide new secure opportunities to facilitate the digital onboarding of customers and non-face-to-face business relationships.[29]

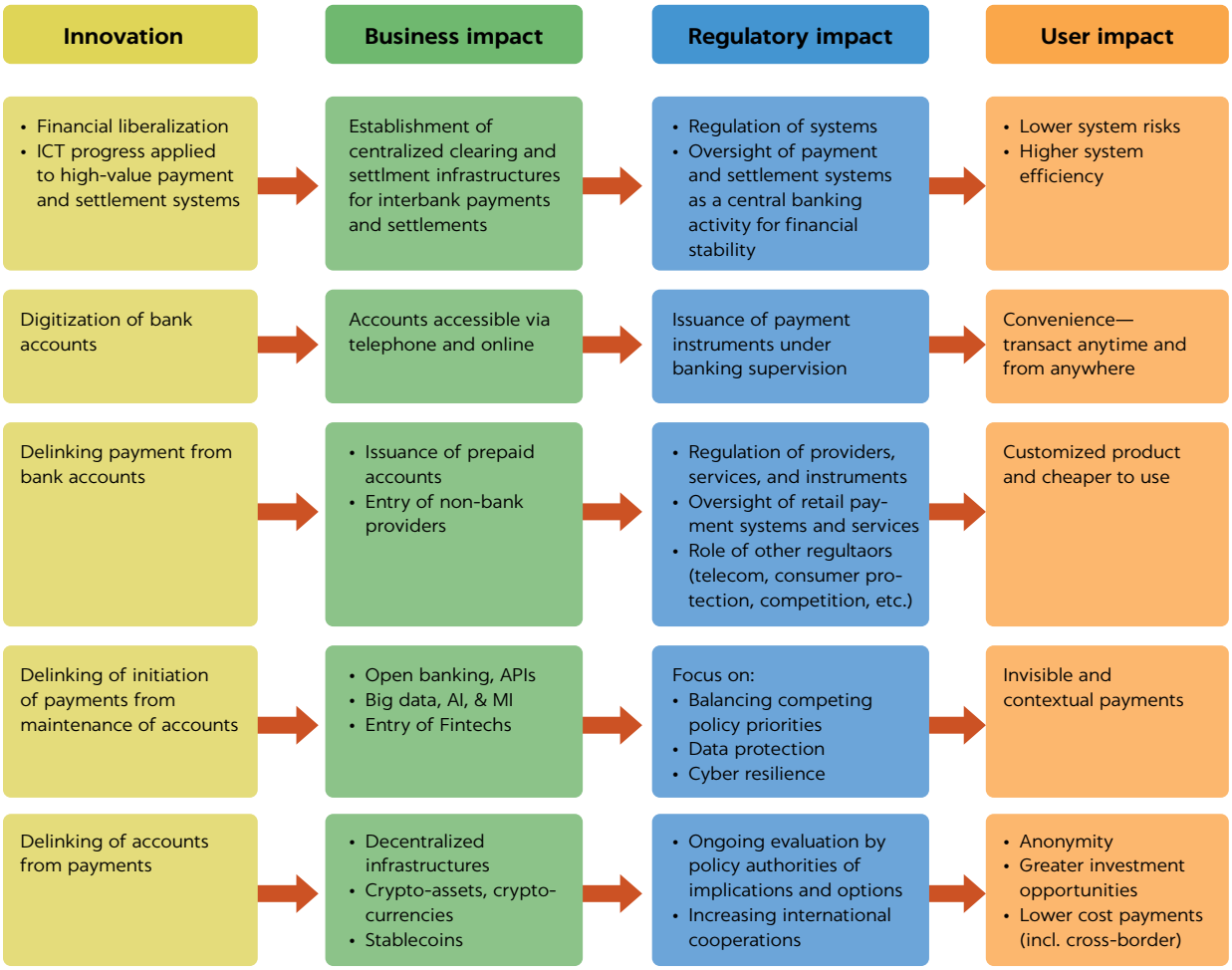
Lastly, the development of DPS, if done incorrectly, may carry its own "risk of exclusion." Trust, capability, consistency, know-your-customer (KYC) regulations, and cost are widely cited as the factors posing the biggest risk to individuals facing financial exclusion (CSJ 2016). As regards trust, evidence shows that, although individuals may technically have access to DPS, their use of these services is influenced predominantly by how, when, where, and by whom such services are provided. Capability, on the other hand, is key in that digital skills are needed for people to access even basic online services. Another facilitating factor is consistency, meaning customers' ability to stay engaged with the use of services, allowing providers to maintain contact and engagement with clients. Another major challenge that increases the risk of financial exclusion is the associated cost of KYC. KYC regulations require DPS providers to collect information and identity-confirmation documents on potential clients, yet for many individuals and households living below the poverty line, these demands cannot be met easily. Finally, the cost of services easily turns out to be too high for lower-income clients and excludes them from their usage. These are costs associated primarily with KYC, sign-up fees, annual fees, and associated expenses.

NEED FOR STRATEGIC DIRECTION AND POLICY ACTION

Developing sound and dynamic DPS ecosystems requires harnessing market forces while mitigating the related risks. Whereas payment business initiatives may arise spontaneously in the absence of established directions and rules, the complexities of an industry like the DPS industry—characterized by constantly changing technologies and an ever-expanding range of players and products—necessitate strategic directions and policy actions by public authorities to create a conducive environment for DPS ecosystems to develop and operate safely and efficiently. This cannot, and does not, happen outside of a consistent set of incentives aimed to ensure infrastructure development, lay the ground for open and fair competition, mitigate risks, and support public confidence in DPS. It thus requires the active presence of a public authority that is capable to set market-friendly rules, supply or catalyze development of critical infrastructures, promote innovation, facilitate stakeholder cooperation where necessary, and ensure that systems and providers perform as expected. The public authorities must be conscious, however, that overregulation or inadequate incentives hinder innovation and discourage market activity; they should therefore confine their action to creating conditions in which businesses can develop without putting themselves, their customers, or the financial system at risk.

Over the years, regulators worldwide have confronted a very challenging task: enabling industry change and adapting to it at the same time. Historically and for a long time, payment services have lain at the heart of commercial banking. Still, up to the middle

FIGURE 4: Evolution of Payments and Payment Regulations



of the *20th* century, as payment technology had not yet progressed so rapidly, payment services were less appreciated than other aspects of the financial system, and issues concerning the provision of payment services were seen mostly as technical matters ("plumbing") to be dealt with by subunits of IT departments within commercial banks. It was not until the mid-1980s, when liberalization started to take ground in countries with more advanced financial systems, that modernization of payment services took on greater weight. Since then, it has increasingly become a key element of financial-sector strategies and policies for most countries everywhere in the world and at all levels of economic development. And the dramatic pace of information and communication technologies has increasingly pushed private-sector agents to adopt innovative technical solutions to serve the increasing demand of their evolving economies for new payment services. As a result, the payment business that for so many years had been the exclusive domain of banks now opened up to a multitude of new (non-bank and, in some cases, not even financial) entities that would fill in the growing market space along an expanding supply chain of services and specialized subservices supporting payments provision, with significant implications for the evolution of regulation and policy (figure 4 and appendix B).[30]

Technology developments have created opportunities for non-bank players to provide new payment service solutions, including, importantly, digital payments. Initially, in many jurisdictions, these new players (for example, telecom network operators) were permitted to operate only through banks (in the context of so-called bank-led models). In fact, a complicating factor (in the area of payments and financial services more broadly) was the inability of many regulators, steeped in a compliance culture based on a rules-based model, to keep up with the rapid rate of change of a (fintech) culture that is often motivated to utilize financial innovation to break norms and override traditional regulatory approaches. As a consequence, there have been (and still are) numerous cases where, due to disruptive innovation, fintech and traditional regulatory models have collided. However, the strong push from both the supply and demand for innovation from the markets and societies has forced regulators and regulations to come to grips with it, and countries have moved (though at different speeds) to upgrade their legal and regulatory apparatus to deal with the pace of change. In an increasing number of jurisdictions, regulations have been adapted to allow non-bank players to become service providers in competition with banks, and new laws and regulations have been enacted to govern the issuance and handling of e-money, with special focus on the need to control its creation, facilitate the clearing and settlement of e-money transactions, protect e-money users from the associated risks, and prevent e-money abuse from criminal activities. Consequently, the various technologies undergirding DPS have steadily gained legitimacy as regulators have focused efforts *on building regulatory frameworks to support new services and processes, while t*he payments industry has greatly progressed in terms of types of instruments to execute fund transfers and range of services made available to customers. From a legal and regulatory standpoint, until recently there have been obstacles in many MENA countries for non-bank e-money issuers to operate (World Bank Global Payment System Survey 2018; World Bank staff assessments). Until recently, non-banks had been allowed to issue e-money independently in only two MENA countries: Iraq and Jordan. In the last one or two years—many of them, in fact, in the last few months—several MENA countries and economies have allowed non-banks to issue e-money independently: Lebanon, Morocco, the West Bank and Gaza, Yemen, Oman, the UAE, Bahrain, and Saudi Arabia.

Regulatory attention is now being placed on standardization as a way to achieve higher service levels, create a level playing field for competition, and encourage innovation. This is a result of the spread of regulatory activity in the more developed markets and is expected to be witnessed in other regions in due course. Moreover, in the wake of the 2008 financial crisis, regulators have focused on systemic risk reduction and financial stability, and their influence has been continuous through the formulation, implementation, and compliance stages of new regulatory requirements and industry initiatives. Regulators have pushed innovation from the supply side through multiple initiatives, such as payments infrastructure modernization and the implementation of faster payment systems (FPSs) and services. Such initiatives are now being embraced by the industry and are being implemented collaboratively by the industry and regulators. In some countries, regulatory frameworks are being introduced that aim to balance private business (profit-making) objectives with public (risk-mitigation) interests.[31]

Currently, one of the main strategic undertakings from regulators is open banking as a way to further foster competition and innovation in DPS markets.[32] As opening customer banking data to third parties through APIs is becoming a global trend, harmonization and interoperability of APIs is taking on greater importance.[33] Regulators are increasingly focused on industry governance and the oversight of new players, and several countries are introducing standards and rules to improve systemic efficiency and safeguard customers (Capgemini-BNP Paribas 2018). Regulations on data privacy and cybersecurity are witnessing significant growth, as regulators recognize the need to protect information integrity to mitigate payment risk and to boost DPS volumes.[34]

Finally, authorities worldwide are concerned about rapid developments in the area of crypto-assets. The authorities' concerns focus mainly on investor and user protection, market integrity, anti-money laundering, bank exposures, and financi1al stability. In recognition of the risks and significant uncertainties surrounding this issue area, strong international cooperative efforts are taking place to monitor and analyze market developments, setting oversight and supervisory expectations for systems and firms, and clarifying how international standards apply to crypto-assets (FSB 2019a). Particular concerns rest on the gaps that may arise when such assets are outside the perimeter of market regulators and payment-system overseers. To some extent, this inevitably reflects the nature of crypto-assets, which may have been designed precisely to function outside established regulatory frameworks. Gaps may also arise from the absence of international standards or recommendations. Also, in recent years, public interest has grown significantly on the introduction of central bank digital currencies as a safe and efficient form of electronic cash.

3

THE MENA REGION: ECONOMY AND DIGITAL PAYMENTS

BASIC ECONOMIC FACTS ABOUT THE MENA REGION

The MENA region is very diverse, with a mixture of many cultures, and its countries and economies vary considerably in terms of economic and financial-sector development. While Qatar and the UAE are at the top of the world list of GDP per capita, Gaza and Yemen rank among the lowest, according to the World Bank's 2018 World Development Indicators. The region shows signs of a "middle-income trap" (Arezki, Fan, and Nguyen 2019)—*the term used in the economic development literature to describe the risk of a growth ceiling for middle-income countries.* Most possibly, one of the factors explaining the trap is the region's slow adoption of general-purpose technologies due to barriers that prevent such adoption in key sectors of the region's economies. According to the World Bank's *Doing Business*, which provides indicators that can be compared across 190 economies, MENA countries are ranked low in starting a business. (For example, in 2019, Egypt is ranked 109th, Saudi Arabia *141st, and Iraq 155th.*) Barriers to entry protect incumbent firms from competition, allow them to operate comfortably in low-productivity activities, limit their trade and economic growth, and reduce their incentives to innovate.

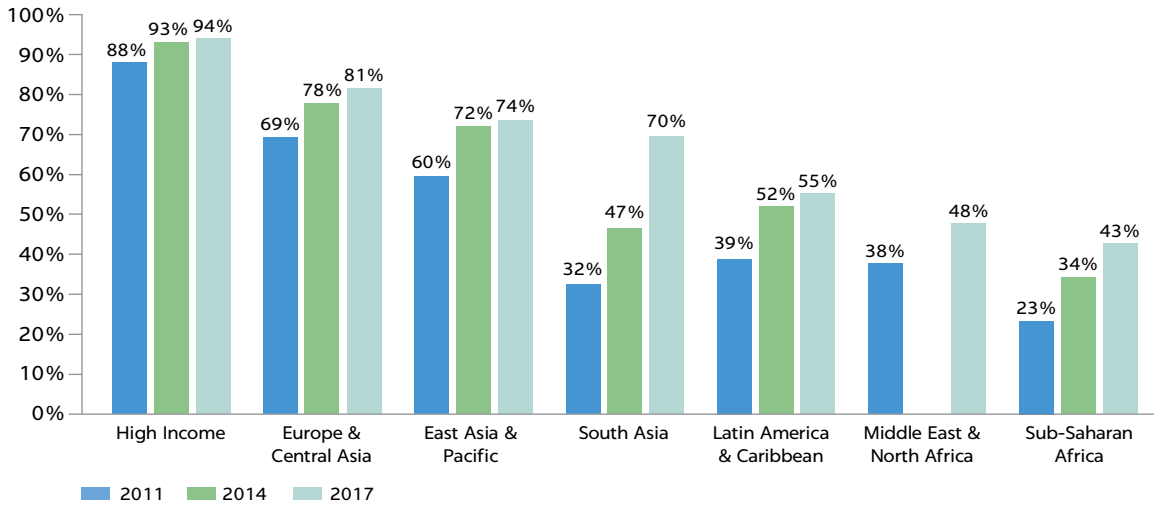
The region has the largest rate of youth unemployment in the world. Data from the World Development Indicators show the highest rates in economies as diverse as the West Bank and Gaza (43 percent), Saudi Arabia (42 percent), Jordan (36 percent), and Tunisia (36 percent), while the countries of the Gulf Cooperation Council (GCC) excluding Saudi Arabia show the lowest rates.[35] Moreover, unemployment in the region features a strong gender connotation; rates among women are nearly twice as high as those for men, reaching 30 percent and beyond in Egypt, Jordan, and Libya against the very low rates in the GCC countries. Overall, financial inclusion has improved, but the MENA region lags behind all other world regions—except Sub-Saharan Africa—and 145 million adults still remain still remain unbanked (figure 5). More specifically, the MENA region performs poorly in terms of employment and financial inclusion of both youth and especially women. In the context of the region's general adult unemployment rate of 9.8 percent (twice as high as the world average), based on the World Development

Indicators, in 2018 the female unemployment rate was 17.7 percent, or 10 percentage points higher than the corresponding male rate. (The difference at the world level is less than 1 percentage point.) Similarly, while total youth unemployment in the MENA region was more than double the world average (26.1 percent and 12.8 percent, respectively), the female rate (38.4 percent) exceeded the corresponding male rate by almost 16 percentage points (2.4 points at the world level). The gender divide characterizes the whole region, as indicated by the data for the MENA region excluding the group of high-income countries. On the financial-inclusion side, Anderson, Hopkins, and Valenzuela (2019), based on the World Bank's data and studies, report that one-quarter of the young population (15–24 year old) in the MENA region hold an account at a financial institution (vis-à-vis 40 percent at the world level), and youth show markedly less ownership of financial accounts than adults. Moreover, ownership of mobile-money accounts among youth in the MENA region remains low (5 percent) and below the world level (15 percent). (See tables C1 and C2 in appendix C.)

The informal economy is widely heterogeneous across the region. Informality is high among non-GCC economies, especially among the young population and in the agricultural workforce. Levels of informality in the region are closely linked to its economic structure and governance climate, including low private-sector vibrancy and limited economic diversification.[36] However, the informal-sector output, on average, amounts to nearly one-quarter of official GDP, lower than in other emerging market and developing economic regions (World Bank 2019).

Banking penetration in the region varies widely. The percentage of commercial bank branches per 100,000 adults, as measured by the World Development Indicators, ranges from 2.6 percent in Iraq to 121.3 percent in Iran, and the percentage of adults holding bank accounts ranges from below 20 percent in Egypt to higher than 90 percent in Iran (ECN 2016). Until recently, financial-inclusion initiatives have been predominantly bank

FIGURE 5: Access to Transaction Accounts (% Adults)[37]

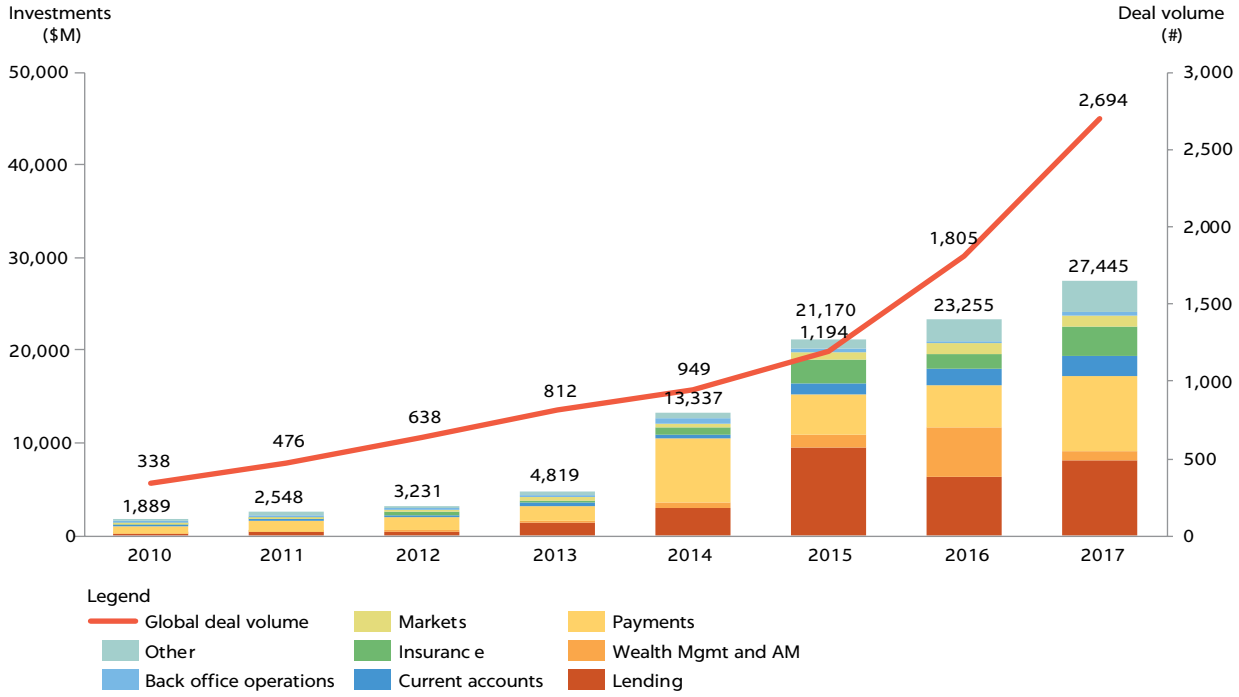


Source: Findex 2017. MENA 2014 data unavailable.

led; participation by non-bank entities and penetration has been limited due to banks' low appetite for risk and asset-heavy model. Mobile subscribers account for 64 percent of the population, yet mobile penetration in the MENA region remains the second lowest in the world, ahead of Sub-Saharan Africa (45 percent) but behind the global average of 67 percent (GSMA 2018). As discussed below, however, this aggregate figure conceals significant variation at the country level.

Poor access to finance is holding back businesses in the MENA region.[38] Several surveys show access to finance as the main impediment to small and medium-size enterprises (SMEs) in the region. While SMEs in the MENA region represent about 96 percent of registered companies and about half of employment, they account for only 7 percent of total bank lending—by far the lowest level in the world. Greater availability of DFS—most notably, better-quality credit information for improved management of SME credit-risk exposures—is recognized to be part of the holistic approach that is required to address this major structural weakness. More broadly, while bank credit remains the most predominant source of SME finance, other financing channels—including SME-specific equity market segments and fintech—can also help serve the needs of SMEs. They could actually be a potential game changer, both by reducing some of the above constraints on bank lending and by opening new financing sources for SMEs, such as through crowdfunding, seed capital, and peer-to-peer electronic platforms.

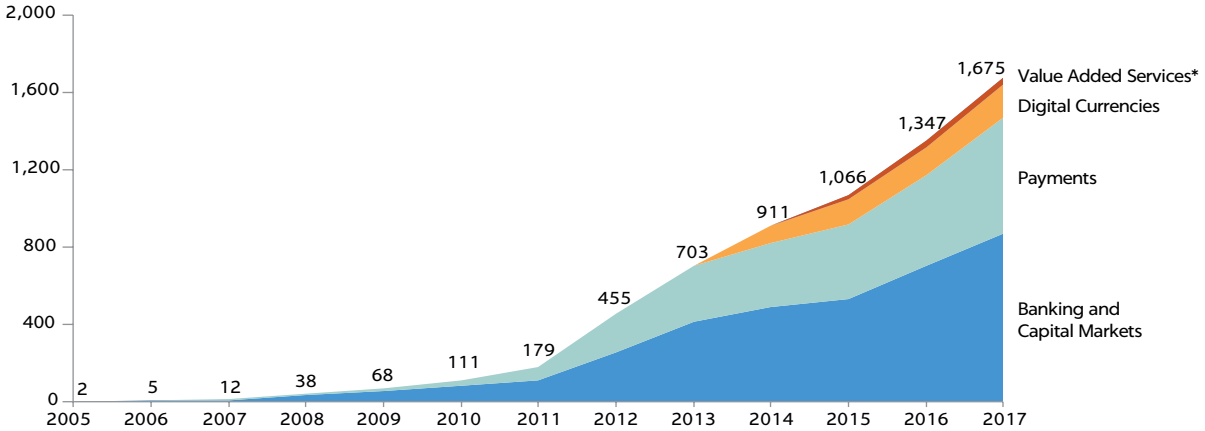
FIGURE 6: Global Fintech Financing Activities (2010–17)



Source: Accenture (2018).

FIGURE 7: Global Fintech Financing Activities (2010–17)

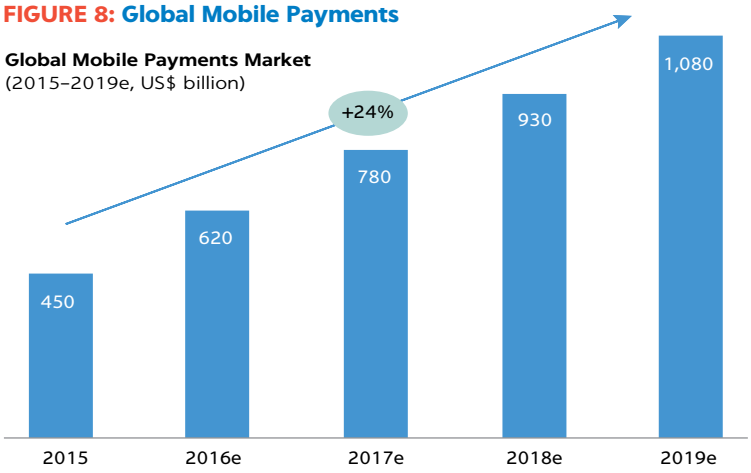
Growth in financial services related APIs, (2015–2017, cumulative, #)



*Value-added services include coupons, rewards, monetisation, marketplace and insurance.

Source: Accenture (2018).

FIGURE 8: Global Mobile Payments



These trends put further pressure on legacy infrastructure and their ability to deliver personalised payments experience.

Source: Accenture (2018).

DPS PROGRESS (I): AT THE REGION LEVEL

Digital finance has spread quickly across the world, and DPS are becoming ubiquitous.[39] Their rapid and global growth (see figures 6–8) has been made possible by the dramatic improvements in mobile network technology and coverage, the greater reliability and sophistication of mobile handsets and digital devices, the higher-quality mechanisms available to identify and authenticate users, the increasing acceptance of digital payment instruments by merchants, and new safe vendor platforms that allow non-bank entities to store and mobilize fiat money-backed stored user value.

Digitalization in the MENA region remains low. Broadly considered, the digital economy accounts for 4.1 percent of the MENA region's GDP, as measured by digital share in private consumption, private investment, government expenditure, and imports and exports. While GCC countries feature more highly digitized economies than their

neighbors, and while they lead the digital consumer charge with very high rates of smartphone adoption and social media usage, the other countries in the region lag significantly behind, and rates in Saudi Arabia, Jordan, and Oman fall somewhere in between. Digital adoption in the business and government sectors remains limited everywhere in the region (the UAE is the only exception), as the MENA region scores low on firm-level technology absorption and per-capita online advertising spending (Digital McKinsey 2016) and governments face considerable implementation challenges (such as inadequate governance structure) in their efforts to digitalize the public sector. Overall, the quality of the Internet connection in the region is poor as compared to the world's other regions (figure 9).

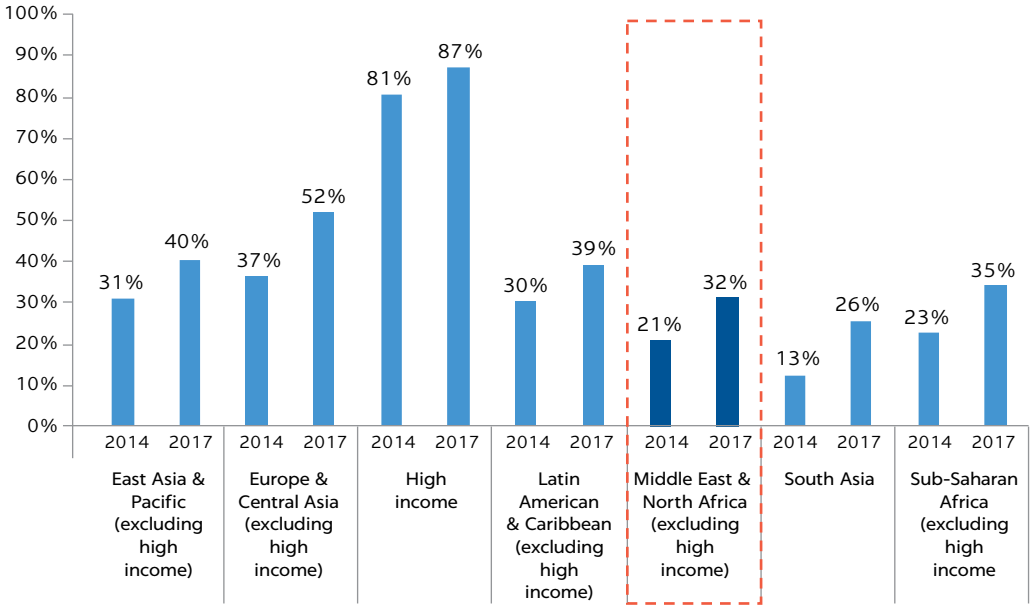
More recently, the region has seen a big push toward digital finance. This is the result of the domestic environment in several countries becoming more enabling, facilitating innovation and bolstering entrepreneurs who seek to exploit business opportunities through new financial products and services. New players, including fintech start-ups, are challenging the status quo and offer customers alternatives to the traditional channels to access finance, and in some countries, a number of players have entered the market for the provision of mobile payment services.[40] The MENA region's fintech start-ups provide services to private, corporate, and governmental partners ranging from payment solutions to marketplace lending and crowdfunding (including for SMEs).[41] In the payments sector, start-ups offer bill payment, mobile and online payment solutions, and wallets. The UAE, Lebanon, Jordan, and Egypt host three-fourths of the MENA start-ups and have established large fintech accelerators.[42] In the MENA region, fintech start-ups have raised more than $100 million in funding in the past decade and over $24 million in 2017 alone, and the current MENA fintech market is estimated at $2 billion and is expected to grow by $125 million a year until 2022 (IFC 2018).[43]

FIGURE 9: Bandwidth Capacity in Bits per Internet User by World Regions

Sources: The Economist Intelligence Unit, Inclusive Internet Index 2018; and World Bank staff calculations.

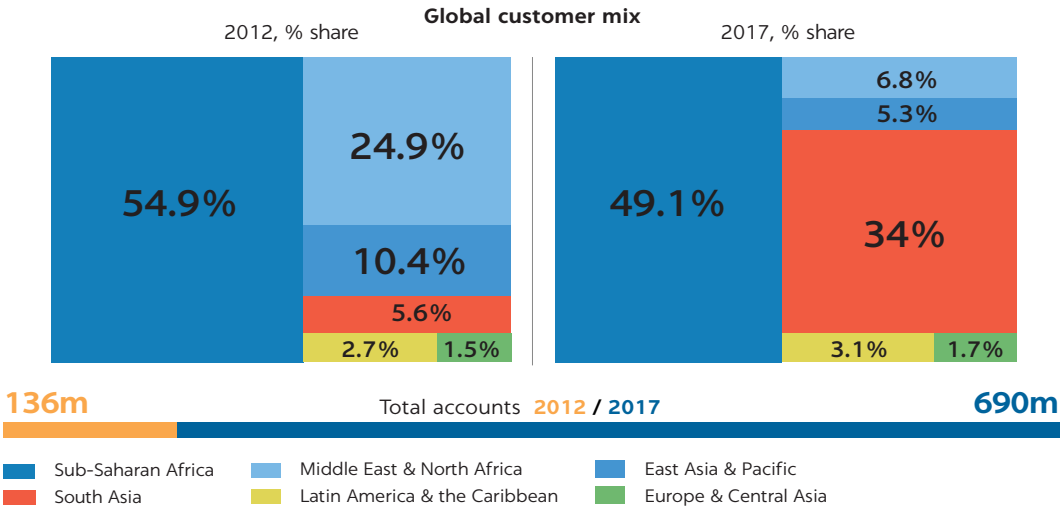
In the area of DPS, however, important gaps remain. The MENA region lags far behind in terms of cashless payments per capita (in 2018, these were 34, while the global average was 78), and the growth in the number of mobile-money customers by region between 2012 and 2017 shows the delayed and tiny progression that still characterizes MENA vis-à-vis other world regions (figures 10 and 11).[44] More broadly, statistics covering the 2014–17 period show that the MENA region has moved from a very low level of digitalization to a much higher level. This, however, still does not compare well with the group of middle-income countries and lags far behind high-income countries (table 1). More

FIGURE 10: Adults Making Digital Payments (by World Regions)



Source: 2018 Global Payment Systems Survey and Capgemini-BNP Paribas (2018).

FIGURE 11: Global Spread of Registered Mobile-Money Customers
(December 2012–December 2017)



Source: GSMA (2017).

specifically, as table 1 shows, the 2017 MENA average (33 percent) is below both the world average (52 percent) and all other country income-group averages—low income (35 percent), lower-middle income (58 percent), upper-middle income (20 percent), and high income (92 percent). The digital payment average for Saudi Arabia (61 percent), the sole GCC country in the nine-country MENA sample, is substantially below the high-income country average (92 percent).

DPS PROGRESS (II): ACROSS THE REGION

The diversity of the MENA region, noted above, is reflected in the different stages of the development of its national DPS ecosystems. Based on a number of indicators, table 2 classifies the development of the countries' DPS ecosystems as *"basic," "evolving," or "innovating,"* to be described in more detail in section IV.B. The indicators have been selected with a view to proxying a number of relevant DPS aspects, including access (differentiated by gender and age), usage, infrastructures, efficiency, and level of financial inclusion. Although data limitation significantly constrains this type of analysis, a number of insights do emerge.

A marked divergence can be observed in terms of access to transaction accounts, both across countries within the region and across genders within countries and economies. Access to accounts ranges from 8 percent in Yemen to 88 percent in the UAE and 92 percent in Iran. Access appears to be correlated with the country level of income, yet it is far lower than the corresponding world averages (by income level). Digital access to accounts (via mobile devices or the Internet) is largely dissimilar country wide. Egypt and Morocco are at the lowest end (4 percent) and way below the world average (34 percent), and the UAE is at the highest end (51 percent). In all countries, the percentage of males (within the male population) with access to a transaction account is larger than the equivalent percentage of females, and the difference is far larger than at the world level. As to the motivation for not holding an account, aside from the insufficiency of funds (which dominates the responses from surveyed individuals everywhere), the most frequently cited reasons in the 2017 Findex are the high cost of services, the lack of necessary documentation, and the lack of trust in financial institutions; religious beliefs and geographical distance from providers did not figure significantly. Finally, regarding access to accounts by firms, the region does not compare unfavorably with the world (80.4 percent and 87.5 percent, respectively); most countries are above the average, while Egypt, Iraq, and Yemen fall substantially below.

Similar strong cross-country and cross-gender divergencies can be found in the usage of digital payments. Using the Findex indicator of people who had made at least one digital payment over the previous year (as a percentage of the adult population), usage ranges from 1 percent in Yemen to 76 percent in the UAE and 79 percent in Iran, again with significant (income-correlated) variability between countries and a strong gender imbalance as compared to world levels. In all MENA countries, male usage is higher than female usage; the difference varies from 1 percentage point in Yemen to 32 percentage points in Saudi Arabia.[45] As regards digital government payments, while the dataset is incomplete, the countries that responded to the survey (mainly high-income ones: Bah-

TABLE 1: MENA (Select Countries) Digital Payments: International Comparison

	Digital Payments Made or Received in the Past Year (% Age 15+)		Mobile-Money Account (% Age 15+)		Used the Internet to Pay Bills in the Past Year (% Age 15+)		Paid Online for Internet Purchase (% Internet Purchasers, Age 15+)		Sent or Received Domestic Remittances in Other than Cash (% Senders and Recipients, Age 15+)		Received Wages into an Account (% Wage Recipients, Age 15+)		Debit or Credit Card Used to Make a Purchase in the Past Year (% Age 15+)	
	2014	2017	2014	2017	2014	2017	2014	2017	2014	2017	2014	2017	2014	2017
Egypt	8	23	1	2		2			32	19	19	34	2	
Iran	4	19		4		40			60		62	84	55	64
MAGHREB														
Algeria	25	26							18	30	74	46	7	3
Morocco		17		1		1				63		36		5
Tunisia	17	29	1	2		3			43	56	33	54	8	11
MASHREQ														
Jordan	13	33				2			16	28	54	44	6	7
Lebanon	32	33	1			6		16	26	50	59	46	20	22
FRAGILE, CONFLICT AND VIOLENCE AFFECTED														
Iraq		8		4		8		9	27			15		
Libya												43		
Syria														
Yemen	3								36					
Saudi Arabia	4	61									60	68	35	47
West Bank and Gaza	16	21				4			23	30	38	30	3	4
MENA		33		6								45		16
World	41	52	2	4		22		73		66	55	62	28	33
Low income	23	35	10	18	3	4			52	67	21	31		
Lower-middle income	42	58	3	5	20	4			47	66	25	34	9	10
Middle income								73	48	63	44	52	19	24
Upper-medium income	27	20	2	4				79	48	79	53	64	27	38
High income	88	92						66			85	87	76	82

Source: 2017 Global Findex Database.

rain, Kuwait, Saudi Arabia, and the UAE) indicated that they have digitized more than 90 percent of their public salary disbursements. The only exception is Libya, at 72 percent.

On payment infrastructures, while all countries possess the core components, only one is at the forefront. All countries in the region except Yemen have a real-time gross settlement (RTGS) system in place, and all (including Yemen) have an automated clearing house (ACH) system that processes direct debits/credit transfers as well as a national cards switch.[46] Only one country—Bahrain—is operating a FPS. Bahrain is also the only country to implement Open API–based payment services.

A varied picture emerges after considering efficiency-related aspects. Using two price-based proxies for efficiency of DPS ecosystems—one payment related (the price of low-value cross-border remittance services) and another unrelated to payments (the bank interest rate spread)—the region as a whole does not differ perceptibly from corresponding world averages, yet the divergences are significant across the countries within the region, suggesting that competition within the banking sector, especially in the lower-income economies of the MENA region, might be a critical determinant of efficiency, as banks may live comfortably on the extra profits they extract from their conventional activities and not face adequate incentives to innovate their payment and financial services.

In conclusion, from considering the evidence just discussed, some general findings emerge. While all MENA countries in the high-income range show advanced DPS features, not all upper-middle-income economies in the region have evolved their DPS in line with their level of economic development (Algeria, Iraq, and Libya are a point in case); on the other hand, lower-middle-income Morocco's ecosystem is evolving dynamically. Also, whereas progress is clearly observable in the region as one moves from bottom up across the different evolutionary levels of national DPS ecosystems, progress overall is still modest relative to other regions in the world.

These findings point to two important conclusions. First, each country of the region should define its own strategy; modernizing the DPS ecosystem requires working at the country level, taking actions that are based on the country's own gaps and challenges. The "multilevel" strategic approach developed in section IV builds on a set of general policy actions that fit all MENA countries but designs policy actions that are specific to each level of evolution of the national DPS ecosystems. Second, working only on the supply side (say, by easing regulations) might not be enough to accelerate DPS development.[47] It is essential that national strategies aim also at the *demand side of DPS provision, through measures intended to increase the capability of consumers to access and use DPS and their comfort doing so.*

TABLE 2: MENA Digital Payments: Regional Diversity (%)

Country	Income Status (*)	Access	Male	Female	Access by Firm	Digital Access	Usage of Digital Payments	Male	Female	G2P	Infrastructures	Open Banking	Efficiency (I)	Efficiency (II)	Non-Banks (E-money Issuance)
Algeria	UMI	43	56	29		5	16	20	11		RTGS, ACH, Switch	No	6.3	9.42 (R)	No
Bahrain	HI	83	86	75		35	69	73	60	93	RTGS, ACH, Switch, FPS (QR code)	Yes	4.2	3.78 (S)	Yes
Djibouti	LMI	15	17	9	91						RTGS, Switch				No
Egypt	LMI	33	39	27	69	4	6	8	4		RTGS, ACH, Switch, FPS	No	6.1	4.90 (R)	No
Iraq	UMI	23	26	20	43	13	11	15	7		RTGS, ACH, Switch	No	7.6		Yes
Iran	UMI	94	96	92		44	79	88	71		RTGS, ACH, Switch				
Jordan	UMI	42	56	27	83	9	14	19	7		RTGS, ACH, Switch, FPS	No	5.0	7.24 (R)	Yes
Kuwait	HI	80	83	73		30	63	66	57	99	RTGS, ACH, Switch	No	1.1	2.24 (S)	No
Lebanon	UMI	45	57	33	93	12	27	34	20		RTGS, ACH, Switch	No	1.2	7.36 (R)	Yes
Libya	UMI	66	71	60		12	21	24	17	72					Yes
Morocco	LMI	29	41	17	97	4	9	13	4		RTGS, ACH, Switch	No		7.47 (R)	Yes
Oman	HI	80	84	64							RTGS, ACH, Switch, FPS (QR code)	No	1.7	4.52 (S)	Yes
Qatar	HI	75	69	62							RTGS, ACH, Switch	No	1.8	5.41 (S)	No
Saudi Arabia	HI	72	81	58		36	57	70	38	91	RTGS, ACH, Switch	No		4.90 (S)	Yes
Syria	LI	25	27	20										13.04 (R)	No
Tunisia	LMI	37	46	28	96		19	25	13		RTGS, ACH, Switch	No		8.59 (R)	Yes
UAE	HI	88	93	76		51	76	81	63	98	RTGS, ACH, Switch, FPS (QR code)	Yes		3.54 (S)	Yes
West Bank and Gaza	LMI	25	34	16	84	8	8	13	4		RTGS, ACH, Switch	No		5.96 (R)	Yes
Yemen	LI	8	11	2	48	8	1	1	0		Switch	No		4.30 (R)	Yes
MENA		43	52	35	80.4	21	23	28	18				5.1	6.91	
World		69	72	65	87.5	34	45	49	42				5.4	6.84	

Sources: 2017 World Bank Findex; 2018 World Bank Enterprise Survey; 2018 World Bank Global Payment Systems Survey; 2018 World Development Indicators; and 2019 World Bank Remittance Prices Worldwide (second quarter).

Notes on Table 2

Full headlines

Access: Adults (at least 15 years old) with access to a transaction account, as a percentage of all adults

Access (female): Female adults (at least 15 years old) with access to a transaction account, as a percentage of all female adults

Access (male): Male adults (at least 15 years old) with access to a transaction account, as a percentage of all female adults

Access (firm): Firms with access to a transaction account, as a percentage of all firms

Digital access to account: Used the Internet or a mobile phone to access a transaction account (percentage with a financial institution account, age 15 and above)

Usage of digital payments (I): Adults (at least 15 years old) who made at least one digital payment during the previous year, as a percentage of all adults

Usage of digital payments (I) (male): Male adults (at least 15 years old) who made at least one digital payment during the previous year, as a percentage of all male adults

Usage of digital payments (I) (female): Female adults (at least 15 years old) who made at least one digital payment during the previous year, as a percentage of all female adults

G2P: Adults (at least 15 years old) who received public-sector wages into a transaction account, as a percentage of all public-sector wage recipients

Infrastructures: Payment systems in operation—that is, real-time gross settlement (RTGS), automated clearing house (ACH), switch, faster payment system (FPS); QR codes used for initiating/accepting faster payments. Card Switch is referenced from a domestic interoperability perspective for card and mobile payments and does not imply a domestic scheme as most MENA countries, with the exception of Syria and Yemen, have many banks issuing payment cards affiliated with international card schemes.

Open banking: Indicates whether a country has adopted the regulatory framework to enable open banking

Efficiency (I): Interest rate spread, calculated as the difference in percentage points between the bank lending and deposit rates

Efficiency (II): Cost of cross-border payments, as a percentage of $200 value (S)ent or (R)eceived

Non-banks (e-money): The country has at least one non-bank financial institution that issues e-money

Criteria that can be used for classifying national DPS ecosystem

The percentage interval for each indicator has been divided into three subintervals of equal size for values ranging from "high" to "medium" and "low." Only the Digital Payments (II) indicator has been divided into two subintervals ("low" and "medium/high"), since it reports a yes-or-no response. For the Infrastructure indicator, the subintervals have been constructed based on the existing platforms: "low" for ecosystems featuring only RTGS and/or ACH systems, "medium" for those also featuring switch(es), and "high" for those featuring fast payments in addition. For each country, the number of "high," "medium," and "low" observations has been counted across all indicators for which data was available, and the highest frequency was used to determine the DPS ecosystem level corresponding to each country. As discussed in section IV.B, the levels bear the following denomination: "basic" for least developed ecosystems, "evolving" for developing ecosystems, and "innovating" for more advanced ecosystems.

4

DEVELOPING SOUND AND DYNAMIC DPS ECOSYSTEMS IN THE MENA REGION

DPS IN MENA: CHALLENGES AND OPPORTUNITIES

The MENA region is capturing only a fraction of its digital potential, revealing significant opportunities for digitalization looking forward. A recent analysis shows that the region's economy has realized only about 50 percent of its digital potential as against the US economy taken as benchmark.[48] Also, looking at the digital supply side from a labor perspective, the analysis shows that the share of digital jobs in the overall regional workforce is significantly lower compared with that of the United States and Europe. A recent survey has identified a number of constraints to fintech growth in the region (IFC 2018c). The primary constraints appear to be at the regulatory and market-access levels, followed by a lack of mentoring support. The absence of an experienced talent pool was also highlighted by the industry. Other constraints include a risk-averse culture, which tends to favor secure jobs against entrepreneurial ones; low levels of financial literacy; limited understanding and/or trust of DFS; limited payment and Internet infrastructures; and limited attention from the media to the fintech phenomenon.

Digital infrastructure in the MENA region lags other emerging regions, and digital payments in some countries of the region see a slower diffusion (Rossotto and Badran 2019). Internet speed is significantly slow. And while Internet access costs have decreased in recent years, they remain high, especially at the bottom of the pyramid. Many Internet markets in MENA countries have monopolies or entry barriers, giving the MENA region the highest Internet market concentration in the world. Entry barriers limit Internet infrastructure development, and this constraint limits innovation across the whole Internet value chain. In addition, new policy challenges are emerging with the growth of digital platforms, and policy makers and regulators in the MENA region may face additional specific challenges. Additional policy concerns are surfacing around the data economy, including privacy and security, and promoting a level playing field across the whole value chain of the data-enabled economy. Mobile broadband uptake in the MENA region is more limited than in other regions, including emerging markets in East and Central Asia. Low quality is also an issue. Most MENA countries have mobile broadband speeds below the global average, and underinvestment in the network infrastructure and limited use of the infrastructure built by network utilities limit growth. Both 4G and

BOX 4 LACKING PRECONDITIONS FOR DIGITAL DEVELOPMENT IN SOME MENA COUNTRIES

The overall picture of technological trends in the MENA region is diverse, as in many respects the levels of development between as well as within most countries are highly uneven. Some of the differences are still growing—for instance, between urban areas with sufficient infrastructure and good dynamism at one end of the spectrum, and, at the other, rural areas with poor infrastructure very static technological development. Factors such as the distribution of basic infrastructure, an enabling business culture, and supportive economic and education policies are different across the region and in its subregions as well. Similarly, governance for innovation (and specifically for information and communications technology) is lacking to a large extent in most MENA countries, with serious gaps in such factors as organizational capacities, regulatory procedures, labor markets, and qualified staff. At the same time, in many other countries and subregions, such conditions are not yet existent.

Other aspects as well are retarding or blocking rapid improvement. In most of the countries and subregions of the MENA region, population growth is relatively high, putting pressure on infrastructures, the labor market, and education systems. Also, not all countries in the region are in a position to offer incentives for foreign corporations to do business there, and even when they are, their attractiveness is often not as high as in some East Asian countries. As a result, foreign investment is often concentrated in specific locations and sectors. Furthermore, while contacts and business relations with actors beyond the region are of utmost relevance to support digitalization, not all MENA countries are linked to institutions from other regions and to advanced countries in the technological realm.

According to the Networked Readiness Index from the World Economic Forum, four indicators appear to influence the readiness to exploit new digital technologies: (1) the regulatory and business environment; (2) infrastructure, affordability, and skills; (3) usage by businesses, individuals, and government; and (4) social and economic impact. Here again, uneven development between and within many of the countries of the region is a challenge.

Overall, MENA economies need greater investment in STEM (science, technology, engineering, and mathematics) subject skills to prepare the younger generation for the demands of the labor market.

Source: Göll and Zwiers (2018).

5G mobile networks need extensive fiber backhaul infrastructure. Other challenges to the development of digital finance are discussed in box 4.

Yet, against this background, the potential is there for a much more rapid pace of digitalization across the region, based on the following factors:

- **DEMOGRAPHY:** More than 60 percent of the MENA region's population is under the age of 25 years. Many youth are tech native and savvy and ready to experiment with unconventional DPS that promise speed and convenience. They are a key source of demand that will boost the MENA region's rate of digital adoption in the coming years. Currently, youth unemployment in conjunction with the current practice of opening a first bank account only when employed hampers adoption of digital services. This shows the need to work on developing DPS that cover the payment needs of unemployed youth and to launch the digital economy as a key employment pathway.

- **INTERNET-ENABLED MOBILES AND SMARTPHONES:** The increasing affordability of mobile phones and decreasing cost of data have resulted in highly digitalized populations across the region.[49] Smartphone penetration ranges from as low as 43 percent in Tunisia to as high as 99 percent in the UAE. The growing penetration of smartphones enables customers to have access to full-fledged payment devices, as opposed to simple communication devices.
- **MIGRATION TO CASHLESS SOCIETIES:** The path to a cashless society varies greatly within the region. The UAE has announced a national goal of becoming cashless by 2020, and the government is creating a DPS environment and setting up supporting infrastructures that are conducive to this goal. In countries where bank accounts are not as prevalent, becoming cashless will take longer, although e-money and mobile-money products could provide an alternative approach, yet even in these countries, some of the infrastructure is already in place, such as connectivity, core payment-system infrastructure, and digital identity document (ID) systems.
- **E-COMMERCE GROWTH:** The rapid growth in e-commerce, especially via social media platforms (for example, Instagram, Facebook, or Pinterest), has created a generation of social media entrepreneurs. E-commerce or mobile commerce platforms have taken off in MENA countries, even though most vendors still operate on a cash-on-delivery basis. The offline-to-online migration is enabling fintechs to tap into the digital trails of merchants (for example, social media footprint, customer ratings/reviews, purchase history) and to make credit decisions based on machine learning algorithms.

The digital adoption gap by consumers, businesses, and governments and the still-low role of information and communications technology imply a strong growth potential for digitalization in the MENA region. It will be critical for the countries in the region to develop the needed technologies and associated human capital. With this purpose in mind, efforts will have to focus on activating the right drivers, including the lead role of the public sector, the engagement of the private sector (and DPS stakeholders more specifically), the buildup of institutional and technical capacity, and the identification of investment needs and sources—all in the context of a comprehensive national strategy. The following section will discuss how strategically to approach the objective of developing sound and dynamic digital ecosystems in the region. The strategic approach formulated below will focus on DPS.

DPS ECOSYSTEMS

A DPS ecosystem consists of various elements. These include the users of DPS, such as consumers, businesses, government agencies, and non-profit groups; the *providers* of DPS, which typically comprise financial intermediaries (for example, banks, savings institutions, credit unions, and other regulated financial institutions), as well as non-financial entities (such as mobile and e-money issuers and operators, postal authorities, technology companies, and a variety of different commercial agents); the *suppliers of support services,* which provide PSPs with all that is needed for the production and delivery of DPS (for example, processors, platforms, software and hardware companies) and include also the agents who work on behalf of PSPs for the delivery of DPS to end

users; and the *infrastructures* that support the production and delivery of DPS, which include the payment systems that allow for the electronic execution of payment and fund-transfer transactions across the economy.

Developing a sound and dynamic DPS ecosystems requires the establishment of a *conducive environment* for DPS provision appropriately conceived of for the given stage of NPS evolution. The environment is defined by the whole set of incentives that guide the behavior of the agents operating in the DPS space and orientate their expectations. The incentives are shaped by the policy authorities (regulators, supervisors, overseers, and so on) with recognized powers to exercise their influence and control over the DPS industry, as well as the policies, laws, and regulations that govern the provision of DPS, the design and standards of the DPS market, the groups and associations reflecting the interests and influence power of the various stakeholders, and the organizations working to promote and support the DPS ecosystem (for example, multilateral agencies, private foundations, donors, and so forth). Other components of the environment are the national strategies for financial-sector development and the strategies for payment-system modernization and financial inclusion. The incentives defining a DPS environment also reflect the quality (in particular, the safety and efficiency) of the technical infrastructures (for example, networks and platforms) for the execution of payments.

The issues faced by stakeholders working to develop a sound and dynamic DPS ecosystem are many and complex. The following list of questions that are to be addressed is only indicative and not exhaustive:

- **REGULATION:** Is the existing legal basis sufficient to ensure sound provision of DPS? Which authorities should be responsible for regulating, supervising, and overseeing PSPs? Would non-financial institutions (for example, social networks) be permitted to provide DPS? How would authorities regulate innovative providers that are not covered under existing regulations? Should PSPs be regulated as an individual legal category, or should regulation be based on the type of services they provide, irrespective of their legal nature? Would PSPs have open access to their supporting infrastructures? Would they operate on a level playing field with incumbents?
- **BUSINESS MODELS:** What are the business models for DPS provision? Are the relevant authorities familiar with these business models and their associated risks? What types of risk-management framework would be appropriate for the new services? Can government agencies champion DPS, thus setting an example through intensive usage of DPS? Can and should government agencies provide DPS to kick-start development? Are the necessary DPS supporting infrastructures in place? Are they interoperable? Which standards should providers adopt for DPS to be delivered safely and efficiently, and how should best practices be communicated and assimilated? *How can DPS users be incentivized to move toward the state of "digital liquidity,"* where they don't limit themselves to cash out the value that is stored in their digital devices and thus use DPS to their fullest potential?
- **USERS:** Why should I open an account? How do I choose a PSP? How do I compare the cost of opening and using an account across different providers? What types of

DPS do I need? How do I select a DPS provider? How safe are they to use? How can I trust a provider? What happens if I encounter a fraud? How do I protect my rights as a consumer? How can I get reliable information and advice?

A REGIONAL STRATEGIC APPROACH

A regional strategy for developing sound and dynamic DPS ecosystems in the MENA region should ultimately enable each country's ecosystem to

Deliver safe and convenient payment services using state-of-the-art (digital) technologies that enable residents to make and receive fund transfers anywhere, to and from any party, at any time, seamlessly and efficiently, including, importantly, under crisis situations.

The strategic approach to achieve these objectives consists of a set of policy choices articulated in "building blocks" and "drivers" framed together in a consistent framework. *The building blocks are the components of a sound and dynamic DPS ecosystem, while the drivers comprise the actions that the policy authorities and relevant stakeholders should take in order to set the building blocks in place and make sure they all fit together and serve their purpose effectively. Both the building blocks and the drivers considered below are* consistent with the typical objectives of NPS modernization and financial inclusion.[50] The consistent (and holistic) application of the building blocks and drivers will also prove critical for reducing the *"risks of exclusion" discussed in section II.A.* In addition, policies will be discussed that maximize the use of DPS to address the MENA region's specific criticalities (that is, the gender divide, limited competition in the banking sector, youth unemployment, and a large informal economy). Finally, taking as an example the COVID-19 crisis, the use of DPS will be discussed for emergencies where physical contact among individuals is restricted or not permitted, yet money flows through the economy and across the whole country and beyond have to be secured to the extent possible.

The strategy focuses on the first three waves of innovation discussed in section II.A—that is, the digitization of bank accounts, delinking of payments from a bank account, and delinking of the initiation of payments from the maintenance of accounts. The fourth wave (the delinking of accounts from payments leading to crypto-assets and cryptocurrencies) comes with many potential issues that are still being studied. In any case, the adoption of the associated DPS is predicated on such issues as KYC, merchant acceptance, agent networks, and consumer protection, which are common to the first three waves. Furthermore, it is not still clear at this stage whether this fourth wave of innovation should be part of an overall strategy for DPS.[51]

However, given the high degree of regional diversity, the approach formulated in this report takes into account the different country circumstances and specificities. In particular, in light of the different initial conditions featured by each DPS ecosystem in the region's countries, the approach is *"multilevel,"* where each level refers to one of the three types of DPS ecosystems introduced in section III and described as follows:

- **BASIC:** Characterized by a relatively undeveloped DPS ecosystem essentially dominated by banks (where most banks offer only basic payment services with minimal attention to Internet banking, mobile banking, and low-income segments), with only few (if any) non-bank PSPs (typically, mobile-money providers) that act mostly through banks; non-interoperable services; some basic government payments provided electronically to civil servants and government social-benefit recipients (at most); significant financial exclusion.
- **EVOLVING:** Characterized by the presence of banks that are active in the payments market or that leave gaps that are filled by non-banks (either competing with banks or in joint venture with them); creation of prepaid concept; online payments mainly associated with bank accounts; introduction of digital access to bank accounts; various digital payment channels and interoperable services available; broad range of recurrent payments (including also to/from government) provided electronically; payment aspects of financial inclusion being addressed via agent banking and/or non-bank PSPs.
- **INNOVATING:** Characterized by sophisticated services provided by a diversified range of PSPs (including also fintechs, techfins, and bigtechs);[52] delinking of initiation of payment from maintenance of account; APIs, big data, and faster payments available; government payments fully digitalized; most residents with access to at least basic DPS.

Note that the features attributed to each of the above levels are only indicative. A DPS ecosystem at one of the three levels does not necessarily have to show all features attributed to that level; in addition, it may show one or a few features that characterize other levels. Also, the indicators used above may not capture effectively all aspects that may be relevant to assess the level of ecosystem development. And, finally, not all of the aspects captured by the indicators should necessarily weigh the same in assessing the ecosystem's level of development.

Note also that the "levels" are defined only broadly. Their d*ifferences are not carved in stone, nor do critical thresholds separate each level from the next.* Yet classifying DPS ecosystems according to different levels of evolution will help in adapting dynamically the policies needed to support their further development. And precisely in *order* to address the idea of continuous adaptation, evolution, and improvement of DPS ecosystems, the strategic approach discussed below is multilevel, in that its building blocks identify pathways from basic to evolving to innovating ecosystems, riding across the whole range of innovative service provision and addressing the gaps along the way. Specifically, in the context of each building block and driver, essential policy actions are proposed to facilitate the transition from the basic to evolving level of DPS ecosystem, while more sophisticated policy expectations and institutions are advised for more advanced ecosystems, to assist in their further development from the evolving to innovating level or directly ("leapfrogging") from the basic to innovating level.

1. BUILDING BLOCKS

The building blocks of the strategic approach consist of a number of strategic actions to support the change of DPS ecosystems. These actions are consistent with the PAFI framework (CPMI-World Bank Group 2016) and the Bali Fintech Agenda[53] and include (i) open-minded regulation; (ii) safe and efficient infrastructures; (iii) integrity and security; (iv) robust competition; and (v) well-protected, informed, and financially educated customers. Strategy success requires as preconditions the existence in each country of solid payment-system foundations, such as a well-founded, clear, transparent, and enforceable legal basis for all material aspects of the system and safe and efficient infrastructures for the execution, clearance, and settlement of transactions.

Regulating with an Open Mind

For DPS to flourish, a legal and regulatory framework needs to be in place that is predictable, risk based, fair, and open enough to facilitate innovation while not compromising risk. Regulation should allow for new entrants, it should be technology neutral, and it should not impose excessive compliance costs on regulated entities. The authorities that are responsible for regulating, supervising, and overseeing the DPS ecosystem should make sure they have the necessary powers, resources, and capacity to fulfill their responsibilities effectively and efficiently. Recently, many jurisdictions have successfully expanded the breadth and reach of DPS through regulations that encourage innovation and open up to a greater role for new non-bank players.

The approach to regulation is critical to determine the preconditions for the takeoff of DPS and their rapid and steady growth. A key question when designing an enabling regulation is market entry, which concerns who should be allowed into the market and under which terms and conditions. Stringent prudential regulations are intended to ensure that PSPs are sound and resilient to shocks and able to invest in the required systems and processes consistent with their product offerings. PSPs should thus be subject to prudential regulation, including requirements for capital and liquidity, governance and organization, and reporting and disclosure. Importantly, individual PSPs may feature different risk profiles (depending on such features as size, types of services supplied, and connectedness with other providers and systems) and should therefore be subject to proportional requirements. Where PSPs, say, offer only low-risk services, full regulation may be unnecessary and even counterproductive to the development of such services. For example, basic payment services such as cash-in and cash-out transactions or small money transfers would not entail credit, liquidity, or market risks and should not fall within the scope of payment-system oversight requirements intended to prevent systemic or system-wide risks. AML/CFT, market conduct, and consumer protection regulations may suffice to make sure that market integrity is preserved against abusive practices from PSPs and that consumer rights and public trust are protected through appropriate transparency and disclosure requirements, standards for customer information, and audit rules.

A lighter regulatory regime would therefore be sufficient to preserve public confidence in the use of these services. Proportionality is especially important for financial inclusion, since unnecessary regulations may raise barriers to market entry and limit people's access to basic payment services for no valid risk-related purpose. In the context of financial inclusion, the concern should be more about the risk that provision of such services would not emerge. The still-weak performance of DPS provision in many countries, due to overly tight regulatory requirements that fail to attract potential providers into the market, suggests that more can be done in the ambit of proportionality.

Another fundamental feature of an enabling PSP regulation is functionality. Regulation should look at the functions of providers, rather than at providers as such. It should thus be designed by the type of service provided by an entity, and not according to the core business or legal nature of the entity providing the service (for example, whether it is a bank, a non-bank financial intermediary, or something else). Functional regulation is necessary to ensure that different entities providing the same type of service are subject to the same set of rules; in other words, it is necessary to ensure a consistent treatment of all the entities that provide the same type of service, irrespective of their different nature or core business. This, in turn, is a prerequisite to enabling all providers of the same type of service to compete (fairly) on a level playing field. Functionality and proportionality are not mutually inconsistent, in that a regulatory framework that is designed for a specific type of service (say, retail payments) could contemplate different (and proportional) sets of rules and requirements for providers in different risk categories—these rules and requirements, though, would have be applied consistently within each risk category. Regulatory approaches that require non-bank PSPs to have a banking license or to form partnerships with banks might impose unwarranted barriers to market entry; such approaches would be disproportionate and nonfunctional.

Finally, regulation should support both competition and cooperation in the DPS ecosystem. The extent to which accessibility and affordability of DPS can be expanded is in part a function of the level of competition among PSPs. Market competition or contestability require, among other things, factors such as greater access to financial infrastructure and the presence of a broad range of PSPs or at least the possibility for new competitors to enter the market without being discriminated against or hampered by incumbents. In this regard, transaction costs must be mitigated. This can be achieved through cooperation by PSPs. Whereas PSPs typically compete directly in the provision of DPS to users, they should cooperate in building infrastructures and in defining and implementing standards due to the specific characteristics of the payment systems where they operate. However, coordination failures do not always make it possible for them to cooperate, thereby introducing inefficiencies and duplications. On the other hand, cooperation may result in collusive behavior by players that have a dominant position in the payments infrastructure. In essence, the focal point is the trade-off between cooperation and competition. In this context, the regulatory framework (and the role of the central bank as overseer of the NPS, to be discussed below) is critical in setting the conditions for inducing PSPs to compete in the provision of ser-

vices and to cooperate on issues of common concern and interest (World Bank 2008). Examples include the establishment by law of fora for policy dialogue, payment-system bodies that work as industry associations of PSPs, the provision for stakeholder consultation and engagement on regulatory and policy issues, and requirements for ensuring interoperability of systems and services.

From Basic to Evolving

Regulators should see beyond banks. Fintech companies, microfinance institutions, mobile-money providers, post offices, and other non-bank players can be instrumental in reaching out to the segments of the population whose needs are not catered to by the banking system. However, they need suitable regulatory instruments to be able to address such needs. The legislation should provide legal backing to the establishment of non-bank e-money issuers that can be leveraged by non-bank financial institutions/companies, smaller financial institutions, and fintech companies willing to provide innovative payment services. Regulatory approval of e-money services should be streamlined and simplified. Regulators should consider enabling regulations to facilitate the provision of API access by commercial banks and other measures creating an enabling environment for open banking. Also, commercial banks, smaller financial institutions, and microfinance institutions should be digitally enabled, so that they can provide their customers with the option to receive loans and pay back the installments through digital payment channels. Branches of smaller financial institutions, non-bank financial institutions, and microfinance institutions should be permitted to act as agents of banks and non-banks providing digital transaction accounts.[54]

In order to facilitate the evolution toward e-money, regulation must fully protect the funds that back customers' e-money holdings.[55] Issuers of e-money hold a positive balance of funds (*"float")* corresponding to the cash or deposits received from users in exchange for the e-money issued to them. Key questions are what issuers should be permitted to do with the funds, and what use should be permitted of the interest income accruing to such funds. As regards the first question, stringent regulation would be necessary to ensure that issuers always have the liquidity needed to pay customers who wish to cash out of the system or to complete the payments initiated by customers and, further, that money is not created by the e-money issuer. (That is, the amount of e-money issued should be equal to the amount prepaid by customers and denominated in the same currency.) This requires funds to be free of risk of loss from poor investment or claims by creditors of the issuers. The funds should be pooled together and held separately ("ring-fenced*" or "segregated"*) from the other assets of the issuers. Specifically, the risk of loss can be mitigated through limitations on the nature of the account that is used for holding the funds. In most countries, the account must be held with prudentially regulated financial institutions (typically, licensed banks); in others, flexibility is granted that permits issuers to invest some of the funds in liquid assets (for example, assets approved by the central bank or government securities). Protection from creditors is achieved by ensuring that the funds are unencumbered (that is, not subject to creditors' claims) and by requiring that the account be an escrow account, a trust, or a fiduciary mechanism (depending on the legal instruments available within the jurisdiction) for the benefit of the users.[56] Regu-

lations must establish additional safeguards to protect the funds in the event that the bank holding them becomes insolvent or in case of misuse or loss of these funds.[57] One of the most common set of risk-mitigation measures that regulators adopt is requiring that PSPs issuing e-money products place the underlying funds in an account at one or more banks, and that such funds be segregated from the operating funds of the PSPs and protected against seizure by creditors and/or the government. In parallel, regulators may decide to impose caps on e-money funds and transactions to reduce the potential size of the loss to holders of e-money accounts and/or for AML/CFT purposes. In addition, regulators may consider various approaches to protect the funds through insurance schemes.[58] Finally, regarding the use of the interest accruing on the float, different rules may apply. The interest income may be used to benefit the e-money customers or the e-money issuers, or for charitable purposes. The issue ultimately is who actually owns the funds and thus holds the right to decide on the use of whatever return they earn from the permitted investments.[59] In China, the People's Bank of China recently required all non-bank e-money issuers to place customer funds in non-interest-bearing accounts with the bank. These measures were implemented in a gradual manner in order to help the e-money issuers to adjust. The rationale for this move appears to be motivating the non-bank e-money providers to build a business model not dependent on the float income.

The authorities' capacity to balance risk and innovation is crucial to support the development of sound and dynamic DPS ecosystems. The authorities should carefully consider the innovations proposed by market players, evaluate their costs and benefits, and assess their compatibility with the existing laws and regulations. They should also understand when existing laws and regulations need to be adapted to facilitate innovations. They should also possess the capacity needed to regulate, supervise, and oversee the DPS ecosystem effectively under the new processes and products, once these are authorized and introduced. As the authorities strive to encourage innovation, they should exercise care to avoid creating excessive, market-distorting "first mover" advantages. Exploiting the experimental phase to learn and design appropriate incentives would help the authorities to prevent or at least contain those distorting effects.

Regulation should be able to give a prompt response to the challenges posed by technological developments. It is important that the regulatory framework is adjusted to the new business realities in a timely manner and does not pose unnecessary and disproportionate burdens on competition while safeguarding the security of the system and the interests of consumers. Delays would compromise the entry of new market players and limit the evolution of the DPS ecosystem and the market's own technological development. Finally, excessive regulatory requirements and heavy bureaucracy—including, for instance, unreasonable duration and paperwork to obtain licenses—should be avoided.

Importantly, regulation should strongly support competition in the market for the provision of DPS. *Given the relevance of this issue, it will be the subject of the dedicated building block discussed below.*

From Evolving to Innovating

As innovation becomes ingrained in a DPS ecosystem, new risks (both idiosyncratic and systemic) need to be identified and effectively addressed in a timely fashion. The policy authorities need to support innovation to harness the many benefits it enables, particularly for financially excluded and underserved groups. They also need to recognize that new risks will be inevitably associated with innovations and that old and new risks need to be mitigated. The authorities can address the innovation/risk trade-off by pushing providers to adopt appropriate risk-management frameworks and standards, developing effective supervisory and oversight tools (including through sharing information with other authorities, both domestically and internationally), and engaging DPS innovators (typically, non-bank entities) and, more broadly, all relevant stakeholders to ensure that risks to consumers, market integrity, public confidence, and financial stability in general are adequately tackled.

New tools may not only streamline compliance requirements for regulated entities but redesign the way regulators deal with innovation, helping them act more flexibly while not compromising risk. Authorities may need to revisit their regulatory, supervisory, and oversight modalities (based on the new digital distribution channels that providers use), revise existing rules, and even allow limited piloting before making any change in their modalities. Authorities may conduct public consultations and establish working groups to evaluate specific topics, or they may create frameworks for experimentation, such as laboratory, hubs, incubators, or sandboxes (see box 5) to determine whether the existing regulatory regime is adequate to deal with innovative services or needs revising. These frameworks allow structured test-and-learn environments to be set up that can enable the development of DPS that meet the needs of customers while limiting potential risks and permitting new and unanticipated risks and challenges to be identified.

The intervention of sectoral regulators should not obstruct, but promote innovation while protecting systems, consumers, and investors, taking into account in particular the risks associated with financial activities. In this context, regulation should be technology neutral, so that the sector can adjust to technological developments. Regulation should aim at providing security, legal certainty, and consumer protection but should open the payment-service markets to innovation and digital market players. This is especially relevant in a context where these operators experience difficulties in bringing to market innovations that enhance competition and consumer choice. New service providers may offer wider consumer choice through DPS, often at lower prices, and the absence of regulation might hamper their potential. The goal of regulation should be to address these developments and create conditions for seizing these market opportunities while ensuring that adequate rules apply consistently to every PSP.

Regulation should facilitate open banking practices. Banks should be required to grant DPS providers access to their clients' account information (upon the clients' consent) via dedicated interfaces (APIs) based on open standards. For example, when a bank client places a payment order through a mobile app developed by a fintech service provider, the client's bank will be obliged to grant the fintech provider access to its client account

BOX 5 REGULATORY APPROACHES TO FINTECHS

Various approaches are available to support digital innovation in finance while mitigating risks using controlled environments.

Innovation hubs or labs provide support, advice, guidance, and even, in some cases, physical office space to either regulated or unregulated firms. They help fintech firms establish their innovation, identify opportunities for growth, and navigate the regulatory, supervisory, policy, or legal environment. They are information-exchange vehicles for fintech matters, through which new companies as well as incumbent institutions with a new technology-driven project can enter into dialogue with the supervisor. Support can be direct and one to one, often in the form of mentorship, or it may be aimed at multiple recipients and does not have to include testing of products or services. Communication between the company and the supervisor usually has an open and informal character. Innovation hubs can range from hosting and attending industry events to informal guidance or assistance in preparing and making an application for authorization or new products. Single points of contact, dedicated newly created units, identified networks of experts, or similar organizational arrangements can be considered as innovation hubs. Supervisors may use innovation hubs to understand and monitor the new business models and technologies and to identify regulatory and supervisory challenges associated with the risks and opportunities.

Accelerators speed the growth of existing companies. They are usually founded and run by experienced private-sector participants. They are fixed-term programs that include funding—usually in exchange for equity—mentorship, or education from the sponsoring partners. Accelerator programs typically involve short, sharp bursts of effort with significant supporting structure and an emphasis on getting a company to a certain level of development. Accelerators aim to help start-ups achieve a level of business growth in just a few months, facilitate the development of projects, and provide start-ups with the tools needed to establish strong value propositions, so they have the best chance of achieving external funding.

Accelerators often facilitate partnership arrangements between innovators, fintech firms, and government authorities, or between established companies and financial institutions. Some central banks and regulatory authorities have developed accelerators where private-sector firms are invited to address specific problems through the application of new technologies—for instance, to see how new solutions can assist in the conduct of supervisory tasks (suptech). Accelerators programs have a set timeframe in which individual companies spend anywhere from a few weeks to a few months working with a group of mentors to build out their business and resolve problems along the way. Mentor networks—which consist of start-up executives and outside investors—represent the largest value added that prospective companies can extract from accelerators. Accelerators start with a very selective application and screening process. Companies are given a small seed investment and access to a large mentor network in exchange for small amounts of equity. At the end of an accelerator program, start-ups participate in a demonstration day attended by investors and media.

Incubators nurture ideas, provide a space in which start-ups can work, and typically offer mentoring, structured services, and investment capital. They typically have ad hoc entry and do not operate on a set time schedule. Incubators assist the start-ups with long-term business development and give them the time and resources needed to design and build efficient and sustainable business models. They seek to transform start-ups at the idea stage into successful self-sustaining businesses. Start-ups entering incubators may be supported for a long time period. While some incubators are indepen-

BOX 5, continued

dent, they can also be sponsored or run by venture capital firms, government entities, or major corporations. Depending on the sponsoring party, an incubator can be focused on a specific market. For example, an incubator sponsored by a hospital may be looking only for health technology start-ups. In many cases, start-ups accepted into incubator programs relocate to specific geographic areas to work with other companies in the incubator. Incubators offer shared space in a co-working environment, a month-to-month lease program, and some connection to the local community. Incubators incubate disruptive ideas with the hope of building out new business models and companies.

Regulatory sandboxes provide safe space for experimenting with new approaches involving the application of technology to finance. They create a controlled (live) environment for businesses to test products with less risk of being sanctioned by the regulator. In return, regulators require applicants to incorporate appropriate safeguards. Eligibility to enter a sandbox is standardized and requires market participants to articulate their added value in a predefined format. This is cost effective for participants and resource effective for regulators. Sandboxes involve face-to-face engagement of regulators with fintech firms. They provide qualifying businesses and regulators with a dedicated communication channel that facilitates their mutual understanding on issues related to financial innovation and helps them to focus on potential challenges early on. Sandboxes are expected to reduce the time to market. Their predefined entry and exit criteria offer greater transparency and replicability than the approaches discussed above.

data for the payment to be made. In principle, every account-servicing PSP, such as credit institutions, should provide at least one API for communication with third-party providers. The relevant documentation and technical specifications should be made available to every authorized third-party provider free of charge, and the API should provide third-party providers and the account holders with the same level of availability, performance, and technical support. The opening up has a series of implications for competition: The ability of third parties to make bank transfers on behalf of customers means that new payment instruments, based on the direct movement of funds between accounts, may compete with debit and credit cards in retail payments, especially online; also, while the movement of funds continues to take place within the banking infrastructure, banks lose the direct relationship that they have with the customer at the moment of payment and become mere providers of the underlying infrastructure. Meanwhile, account information services, which aggregate data from the customer's transactions with various entities, increase the comparability between payment account services and reduce for consumers the cost of switching from one provider to another by offering a common repository of their transactions. As is the case with payment-initiation services, account information services serve as interfaces between the customers and financial institutions, reducing the direct relationship between the two. Open banking can be implemented through competition law or sector-specific regulation to mitigate the market power of digital platforms.

Regulation should similarly facilitate the use of big data while protecting the DPS ecosystem from abuse.[60] *Big data is affecting all industries worldwide, and even more the payments business. The increased collection, analysis, and sharing of payments data could drive innovation, resulting in more payment products and services being available to end users. It may help predict which payment method would be more successful on a specific transaction, and it can play a pivotal role in predicting fraud and insolvency.[61] In addition, big data may support the payments industry by forecasting churn from customers and by improving and automating both KYC and customer service. Yet it can also influence how companies gain competitive advantage, which could ultimately affect market structure and the nature of competition in the sector, potentially resulting in end users getting a reduced range or quality of services. Regulating big data inevitably involves not just the DPS overseer but also the national competition authority as well as data-integrity and information-securities agencies, where these are present.[62] Also, the commercial use of personal data extracted from payment activities requires legal protection and oversight, as discussed in section II.*

Moreover, there are many uses of big data beyond the payments space (including, for instance, creditworthiness assessment, risk assessment by insurance companies, investment, financial guidance and advice, and so on). Likewise, payment services today may be embedded in the provision of other financial services. Also, the use of new information technologies may increase the risks of cyberattacks, and violation of privacy rules could add growing concerns if PSPs provide other financial services beyond payments (for instance, banking services), thus making necessary improved cyber mapping, reporting, and possibly new regulation. All this implies that the DPS overseer cooperate closely with all other relevant (financial and non-financial) regulators with a view both to facilitating innovation and to dealing with its associated risks. (See the discussion on cooperation in subsection 2 below.)

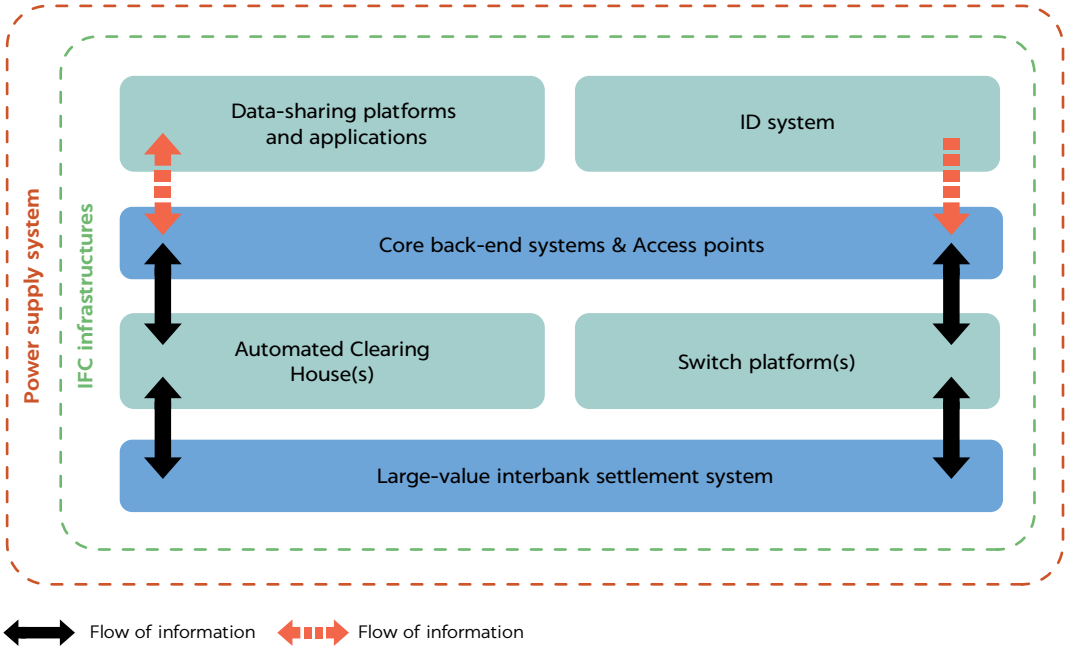
Setting Up Safe and Efficient Infrastructures

Safe and efficient infrastructures are needed to enable effective delivery of DPS (figure 12). Infrastructures consist of the multilateral systems (including also their operators and participants) that allow for the secure and cost-effective execution, clearing, settling, and recording of transactions. These infrastructures establish sets of common rules and procedures for all participants and provide technical platforms as well as specialized risk-management frameworks that enable PSPs and users to transact conveniently and at low risk. It should be noted that technological improvements may allow countries to leapfrog from basic to innovating on the infrastructure dimension. As an example, the so-called automated transfer systems currently in use in many countries bring together real-time gross settlement and ACH platforms, allowing even least-developed economies to jump to frontier interbank payment facilities and to benefit from their highest safety and efficiency standards. Now, one can easily imagine all-in-one payment systems combining real-time gross settlement, ACH, and faster payments, or ACH and faster payments, or else card payments and faster payments, tokenization, and other latest-generation payment features.

The success of DPS usage depends critically on the availability, quality, and reliability of access points. *Limited access to either in-person or remote payment facilities reduces the likelihood that DPS are adopted and actually used.*[63] *National public authorities committed to developing DPS should therefore take a strategic approach to payment infrastructures (and related components) that are needed to support DPS delivery. To this purpose, where feasible, the authorities should always leverage the country's strategy for modernizing its payment system and financial-inclusion agenda. (See section IV.C.)*

A strategic approach to DPS development requires the policy authorities to work closely with the private sector. Such cooperation ensures that the entire ecosystem for DPS runs smoothly and seamlessly, from payment systems to voice and data networks, networks of point-of-sale (POS) terminals and ATMs, and the power systems that underpin these networks. In fact, a reliable supply of electricity is vital to DPS.[64] Similarly, new technologies such as QR codes provide good examples of seamless, light, and cost-efficient methods of initiating and accepting digital payments. Since the provisioning and ownership of the DPS ecosystem requires a combination of public and private resources, policy authorities need to take care to evaluate the options of relying solely on private investment, activate a public-spending program on infrastructure where needed, use targeted subsidies where warranted, and/or adopt legal mandates to service providers where this is deemed necessary for the public good.

FIGURE 12: DPS Infrastructures



Source: Re-elaboration of the PAFI model (CPMI-World Bank Group 2016).

From Basic to Evolving

Efficient and effective infrastructures are needed to facilitate the diffusion of DPS provision. Key infrastructures for DPS delivery comprise the following: payment systems for transactions between and among end users and providers; ACHs and switch platforms and scheme management for the processing of e-money transactions; identity and authentication systems to identify users and providers and to recognize and validate these identities (box 6); and the network of access points for individual customers such as ATMs, POS terminals, branches, or agents (box 7).[65]

Other infrastructures play a critical role in supporting the evolution of the DPS ecosystem. These include platforms to exchange information, such as the voice and data communication networks to support financial messaging between users and providers, and their related applications. They also include the PSPs' core back-end systems to process daily payment transactions and to post updates to accounts and other financial records, with interfaces to general ledger systems and reporting tools, bill-payment platforms, and the underlying communication networks that support all these systems.[66] The policy authorities should also invest in building broadband infrastructure, in particular to extend services to rural areas that are not economically feasible for private players.

An area of particular relevance is *access* to infrastructures. The authorities have to make sure that such infrastructures are accessible. PSPs must rely on network operators for accessing networks, since they may often be both users and competitors of the network operators—as, for instance, when mobile network operators (MNOs) also offer mobile-money services. This potential conflict of interest exposes PSPs to the risk of facing access restrictions by MNOs. This risk may be serious when MNOs are a concentrated market. MNOs that are dominant in the mobile telecommunication market and aspire to grow in the mobile-money services market (or to protect their position in it) may have both the ability and the incentive to exclude competitors from the mobile financial services market or to increase their costs. As with the harm to consumers from dominant providers that operate exclusive agent networks, the harm from MNOs to competing PSPs includes weaker innovation, a narrower range of available services, and higher prices.

Access criteria should be clear, objective, proportional, non-discriminatory, and publicly disclosed. *Fair* representation of participants in the governance of the infrastructures should be encouraged. Governance should ensure that the different needs and interests of the diverse stakeholders are reflected appropriately and that mechanisms are set up for sharing relevant information and for stakeholder consultation and dialogue. The governance process should foresee effective dispute-resolution mechanisms and the orderly exit of participants without unreasonably disrupting the infrastructure.

BOX 6 FACILITATING CUSTOMER IDENTIFICATION

PSPs must be able to access customers' personally identifiable information. Although part of the national information and communications technology infrastructure, the importance of a national ID system for DPS deserves dedicated attention. A national ID system supports DPS delivery by authenticating the identity of DPS customers, ensuring their uniqueness, and meeting customer due-diligence requirements. In addition, the national ID system can be used to cross-reference IDs to PSP accounts, and national ID cards may double as payment cards, freeing PSPs from having to handle transaction-account details. An efficient national digital ID system is therefore essential for the effective delivery of DPS. Such a system should cover all of a country's citizens (as well as resident individual and legal persons); also, it should be able to issue uniquely numbered IDs that are not easy to falsify or duplicate, it should be easily queried, and it should support quick and easy account-opening procedures. National governments should prioritize the availability of a robust and easily verifiable digital ID (whether biometric or another data-based type), which can be used to facilitate access to DFS. Concerns about privacy and civil liberties need to be addressed.

While, in principle, all citizens of a country should be entitled to a national ID, in practice, the poor and vulnerable are significantly less likely to hold a national ID than the general population. In fact, the requirement to hold a national ID can cause exclusion, while gaining a national ID provides benefits far beyond the ability to access DPS. This approach would well serve the broader purpose of achieving social and economic inclusion. Regulators increasingly recognize that weak (or nonexistent) official ID systems act as a major barrier to the inclusion of all members of society. Some regulators are taking measures to address the problem by introducing special-purpose ID systems that can be useful in the interim in the absence of universal-coverage ID schemes. National authorities, donors, and other stakeholders worldwide are taking initiatives to assist in the establishment of comprehensive ID programs in developing countries, to enable access to financial and multiple other types of services. The *Principles on Identification for Sustainable Development*, launched by the World Bank-hosted Identification for Development initiative and endorsed by many global organizations (ranging from development agencies to think tanks and industry groups), set out guidance to help facilitate the development of robust and inclusive digital ID systems (Principles 2017).

BOX 7 BUILDING AGENT NETWORKS

Where users are remotely located, agents are PSPs' direct human interface with their customers. Agents conduct client transactions on behalf of PSPs under a valid agency agreement. As with branchless banking, agent networks enable non-bank PSPs to have far greater coverage than brick-and-mortar bank branches and to operate without their capital and operating costs. Besides, in order to achieve the necessary scale and for network economies to take off, non-bank PSPs rely on agents to deal with their customers more proximately and to gain their customers' trust.

PSPs should be given flexibility to use agents the way they deem fit, based on their business model, provided they carefully manage the associated risks. Risks may involve, among other things, fraud, theft, illegal service provision, counterfeit money, and lack of liquidity, as well as poor explanation of the service, lack of claim-redress mechanisms, and errors. Therefore, regulators typically limit the delegation of customer-facing functions from PSPs to agents. For example, they may require that agents be registered legal entities with a business license or a minimum amount of capital, and that PSPs be liable for the conduct of the agents. Regulators also commonly require PSPs to carry out due diligence on their agents when selecting them, to notify the regulator of their appointed agents, to train them (not only to provide agent services but also to maintain a sound market conduct), and to supervise their activities. Thus, PSPs act as the intermediaries between the regulator and the agents as customer interfaces. In fact, in many countries, regulations have proven to be excessively demanding on the agents and their principals, discouraging the use of agents by PSPs or affecting the business case for prospective agents and thus failing to attract them to the market. Over time, as the risks associated with agents have become better understood and they have been weighed against the opportunity to drive financial inclusion, regulatory requirement for agents in several jurisdictions have rightly been revised and lightened. Provided that risk-management responsibilities are adequately allocated and enforced, PSPs and agents should be given ample latitude to identify the activities and to negotiate contractual terms and conditions that can best serve their purposes and improve their business prospects. This would permit PSPs to increase the geographic coverage of their services at lower cost and encourage competition in DPS provision. Greater competition can be expected to drive financial inclusion to people who otherwise would be left without access to payment services.

The PSP that is able to establish the widest coverage of agents gains a significant competitive advantage over entrants that still have to grow their agent network. Building an agent network involves substantial up-front costs for recruitment and training, running costs for commissions and supervision, and the cost of transferring know-how. Firms that make such an investment need to recover their investment and therefore have an interest in seeing that competitors do not get a free ride on their investments by engaging the same agents. This typically leads firms to protect their investment by adopting exclusivity arrangements, whereby they require agents to act exclusively for them. Yet this may become a major impediment to the ability of competing PSPs to build a viable rival business and result in a lack of competitive pressure on the leading PSP to improve quality and variety in its services.

Moreover, as network effects take root, the unavailability of agents may consolidate market leadership and lead to a single dominant player.

One way of resolving the economics of agent use by multiple PSPs would be to allow an agent that is contracted by a PSP to offer the products of other PSPs provided that the PSPs using the same agent share the costs associated with agent management akin to, say, interchange fees. In such

BOX 7, continued

an arrangement, the service would be available to customers at the front end, while agent charges and cost sharing would be transparent to customers and would be tackled at the back end. However, the principal who has contracted the agent would be liable for all actions of the agent, including where the services are provided by the agent in an interoperable environment for other PSPs. This would be akin to the ATM and POS terminals. If regulators decide to prohibit exclusivity arrangements, the enforcement and publicity of such prohibitions is important, as agents of leading PSPs may be under pressure from their principals not to become agents of competing PSPs.

Access criteria should ensure a level playing field among market participants. The criteria should be justified in terms of the safety and efficiency of the infrastructure and the broader financial system. They should aim at minimizing legal, financial, and operational risks and require participants to possess the operational capacity, financial resources, legal foundation, and risk-management expertise to manage and mitigate risks adequately. Access criteria should have the least restrictive impact on access that circumstances permit, and they should be commensurate with the risks that participants may face and pose. Where feasible, regulation should allow non-bank PSPs to choose to have direct access to the clearing and settlement infrastructures, provided they meet the authorization requirements. Large non-bank PSPs, in fact, should be expected or even required to request direct access to such infrastructures. Access criteria should be applied on an ongoing basis, and compliance with them should be monitored by the relevant authorities through the receipt of timely and accurate information. If compliance is no longer satisfied, rules and procedures should be legally set either for inducing corrective action from the participant, for sanctioning noncompliance, or for suspending or even terminating participation. If an applicant is denied access by a system owner or operator, the reasons should be explained to the applicant in writing on the basis of the access criteria adopted.

As a matter of principle, regulators should promote and foster *interoperability* of services and systems.[67] *In fact, to the extent that the infrastructure available allows for it, and consistent with the incentive structure for PSPs (see discussion below), the authorities should strive to achieve account-to-account interoperability and interoperability at ATMs, agents, and merchants. DPS* operate through accounts, whether e-money or bank deposit or credit/loan accounts. Account-to-account interoperability is the ability to transfer funds from one account to another.[68] It enables transfers between customer accounts at different PSPs and between accounts held at PSPs and those held at banks. Such interoperability is necessary for users to conduct electronic payment transactions with any other user in a convenient, affordable, fast, seamless, and secure way via a single transaction account, irrespective of which provider or network they used.[69]

Synchronizing the entry of non-bank players and the development of interoperability arrangements might be particularly challenging for countries in the basic stage of DPS development. A recommended approach for such countries is to lay out the regulatory expectations of interoperability, to focus on building consensus and buy-in from the industry on interoperability, and to facilitate and foster the development of interoperability arrangements. However, for countries possessing institutional structures and infrastructures that can be harnessed for the interoperability of new payment services, it might be advisable to insist on interoperability from the beginning.

From Evolving to Innovating

In the short term, authorities might not insist on interoperability in basic DPS ecosystems (where existing infrastructures do not support it); however, interoperability should be a must for those ecosystems that are already at the evolving or innovating level. *Here, PSPs should be required to adopt common and open messaging and communication standards that allow for different technological communication solutions and the use of different types of devices.* Where interoperability is not in place, it can be very difficult for PSPs to build market share after the first mover has attracted a critical mass of customers.[70] Providers typically allow interoperability between different accounts of the same individual and between accounts of different individuals with the same institution. While there is extensive interoperability among bank accounts in most countries today, interoperability between bank accounts and e-money services, as well as between e-money services of different PSPs, is not the norm. Most PSPs still allow transactions only between accounts belonging to their own subscribers (*"on-net" or "on-us" transfers)*. Without interoperability, large banks and larger non-bank players such as MNOs may gain a disproportionate competitive advantage and use this advantage to prevent their competitors from growing their market share.[71] If customers of the largest providers cannot send and receive money to and from providers that have a smaller subscriber base, the latter are less useful and attractive to customers, and it can be very difficult for alternative providers to build market share after the incumbents have attracted a critical mass of customers. Besides, the lack of account-to-account interoperability inflicts inconveniences and inflexibility on users. Interoperability requires transactions to be authorized and processed in real time (though not necessarily settled) and charges for cross-network transfers to be kept as low as possible and not significantly higher than those applying to in-network transfers.

Interoperability is multilayered, and authorities should consider calibrating the scope of interoperability in line with the needs in the market and stage of infrastructure development. Interoperability as a concept is straightforward—essentially allowing wide usage of a given payment instrument or service across different service providers. A careful analysis, however, reveals that there are multiple{-two?-} layers. The *first layer* regards the type of *underlying transactions*—that is, across which transactions is a service interoperable? The *second layer* refers to interoperability for the same type of payment instrument or across payment instruments (for example, interoperability of credit transfers between bank accounts, between mobile-money accounts, and between bank accounts and mobile-money accounts).

Interoperability at its core requires standardization, infrastructure to exchange messages and instructions between providers (often called a "switch"), a set of business rules (referred to as a "scheme"), and finally an arrangement for clearing and settling transactions (referred to as the "settlement system"). The switch, scheme, and settlement system could all be operated by a single institution or by different ones, and the same switch could support multiple schemes. Similarly, a settlement system could support multiple schemes. This gives rise to the notion of multiple levels of interoperability in each of the layers described above—at device level, intra-system-wide, and cross-system-wide. In device-level interoperability, there is standardization of the processes as well as of physical and technical aspects, such as the size of a debit card, the location of the chip on the card, and the process of interaction between a card and a POS device. This level of interoperability allows, for example, an agent to use the same device to service customers of different PSPs with whom the agent has an agreement. Another example could be for a PSP to use the same device (say, a POS terminal) to participate in multiple switches and schemes. Intra-system-wide interoperability means interoperability among the participants of a particular system. A classic example of this is the case of Visa or Mastercard: All Visa cards are interoperable at all Visa ATMs, but a Visa card cannot be used at an ATM that is managed by a PSP that participates only in Mastercard. It should be noted, however, that as there is device-level interoperability in the cards space, a PSP that is a member of both Visa and Mastercard can support customers of PSPs affiliated with both cards. The last and ultimate level of interoperability is the notion of cross-system interoperability; this requires interconnections between different systems.

Interoperability can be negotiated among PSPs or imposed by the regulator. Voluntarily negotiated interoperability may be hard to achieve since it requires PSPs to undertake costly adaptations to their systems and, most importantly, since large PSPs with extensive infrastructure and up-front investment in networks may see no incentive to volunteer to interoperate with competitors and may not wish to surrender protections of their market share. In some cases, voluntary solutions have evolved as market players have recognized that interoperability was in their own commercial interest.[72]

If it is not market led, interoperability may be difficult to implement even when it is imposed by regulation. *Policy authorities may need make an effort to facilitate negotiations among participants.* Indeed, moral suasion from the authorities has worked well in several countries (for example, in India and Egypt) in order to bring the market players together and catalyze market-led interoperability.

Regulators need to balance the risk of requiring interoperability too late against the risk of intervening when the market is not ready. Introducing interoperability too early may be counterproductive if it lessens the incentives from network effects for first movers; also, imposing interoperability while there is extensive experimentation with new business models may reduce the incentives for innovation and investment. On the other hand, as markets mature, leading firms may develop network effects so strong that even the best competitors cannot make any headway due to market dominance, and where a single provider is dominant, network effects can crowd out competition and entrench the current market structure.

There is a risk that without interoperability, or if interoperability is introduced too late, market leaders may become entirely shielded from competition. Interoperability is essential to alleviate harmful network effects, and regulatory intervention is necessary when no market-driven solution leads to interoperable services. That is why interoperability may be a matter of choice when the DPS ecosystem moves from basic to evolving (and the authorities may well confine themselves to consider it as an expectation and prepare the ground for it, rather than impose it as a requirement), but it becomes a "must do" for the further evolution of DPS.[73]

Interoperability (as for open banking) can be implemented through competition law or sector-specific regulation to mitigate the market power of digital platforms. DPS are characterized by sunk costs in infrastructure, strong network effects, and winner-takes-all (or winner-takes-most) dynamics that typically hinder the appearance of new players or the growth of smaller companies. In this context, promoting or even mandating interoperability may prove necessary to maintain competition in DPS markets.[74]

Finally, telecommunications network infrastructures matter more and more, in particular for economies moving from the evolving to innovating level. As PSPs increasingly turn to technologies like 5G telecom networks and introduce the Internet of Things and other innovative technologies into daily life to improve the customer experience and gain market share, harnessing the potential of these at scale depends on progress made with a country's overall telecom and networking infrastructure. Increased bandwidth may enable further innovation in payment and financial services. Other technologies, such as cloud computing, would also be relevant to enable new entrants to scale rapidly and grow their penetration. Cloud computing in turn is conditioned on a reliable and high-speed telecom infrastructure.

In the context of innovating ecosystems, growing importance is given to facilities for the delivery of fast payment services.[75] In most countries where fast payments have been implemented, the payments industry was initially driven to implement an FPS as a result of a government mandate or regulation. In some countries, central banks own and operate FPSs (for example, Iceland, Mexico). In other countries, private operators—often owned by major banks—offer fast payment services (for example, Australia, Japan, Sweden, and the United Kingdom). Table 3 reports examples of countries with different FPS models. Even in countries where private operators provide authorization and clearing services for faster payments, settlement services are typically provided by the central bank. Most countries have initially focused on providing faster person-to-person payments and/or business-to-business payments. Since these types of payments are frequently made today by checks or cash, faster payment options provide opportunities for greater payment efficiency and enhanced data capabilities. Many countries that originally built FPSs using domestic messaging standards, with limited ability to transmit detailed payment data and/or limited cross-border interoperability, have since decided to transition to more flexible messaging standards, while others have designed new payment systems with improved data and e-invoicing capabilities in mind, allowing businesses to streamline their accounting systems and

TABLE 3: Indicative CPMI Countries with Different FPS Models

Country	Operator	Clearing Participation Model—Banks	Clearing Participation Model—Non-banks	Settlement Participation Model—Banks	Settlement Participation Model—Non-banks	Inter PSP Settlement Model	Access Channels
Korea	Financial Telecommunications and Clearings Institute	Direct	Direct	Direct	Indirect	Deferred net	Online, mobile, physical channel
South Africa	BankservAfrica	Direct	NA	Direct	NA	Deferred gross	Online, mobile, physical channel
United Kingdom	Faster Payments Scheme Ltd.	Direct	Direct	Direct	Indirect	Deferred net	Online, mobile, physical channel
China	People's Bank of China	Direct	NA	Direct	NA	Deferred net	Online, mobile, physical channel
India	National Payments Corporation of India	Direct	Direct	Direct	Indirect	Deferred net	Online, mobile, physical channel
Sweden	Bankgirot	Direct	Indirect	Direct	Indirect	Real time	Mobile
Turkey	BKM	Direct	NA	Direct	NA	Deferred net	Mobile
Italy	SIA	Direct	Indirect	Direct	Indirect	Deferred net	Online, mobile
Singapore	Banking Computer Services Pte. Ltd.	Direct	NA	Direct	NA	Deferred net	Online, mobile, physical channel
Switzerland	Twint	Direct	NA	Direct	NA	Deferred net	Mobile
Mexico	Bank of Mexico	Direct	Direct	Direct	Direct	Real-time	Online, mobile, physical channel

Source: CPMI (2016).

automate business processes. In addition to the growing number of national-level FPSs operating around the world, there is also a movement toward greater cross-border interoperability between systems.

Finally, integration of the regional payment infrastructures should be promoted. This is not just about linking or integrating technological platforms from a technical standpoint; it is equally about harmonizing and defining a common legal and regulatory framework for transacting, clearing, and settling cross-border transactions, including operating rules, business practices and standards, participation requirements, and funding schemes. The forms of integration at the regional or cross-regional level can range from relatively simple agreements among service providers to facilitate direct or indirect cross participation, to interoperability arrangements involving technical interfaces between the separate operating platforms, and to full harmonization of the operating schemes and integration of the technical platforms into a common unified system for dealing with cross-border transactions. Traditionally, cross-border payments across the Arab region have relied largely on decentralized bilateral correspondent banking relationships to send and receive payments between two member countries, often entailing settlement through correspondent banks outside the region. Several inefficiencies have resulted from these arrangements, such as longer end-to-end processing times, higher costs and variability in liquidity requirements, and potential reductions in economic integrations, among others. The Arab Regional Payments System, which was launched recently, can provide a viable solution and should be pursued as part of the strategic effort to facilitate the development of regional cross-border DPS.

Strengthening Integrity and Security

Payment systems are exposed to risks of integrity and security from criminal activities. These include fraud, financing of terrorism, money laundering, and information abuse and emanate from individuals or entities exploiting the weaknesses of the systems, such as the anonymity of payments, the difficulty of tracking them (due to pooling of funds and delegation of functions), the speed with which transactions occur, and the difficulty of monitoring the systems. Regulation should require licensed systems and PSPs to manage such weaknesses in order to control the above risks through a combination of the following measures:

- *Customer due diligence* (CDD) requirements to gather sufficient information about customers[76]
- *Strict security requirements* for online payment services and increased consumer protection in digital payments and transactions through strong authentication procedures to identify customers when transacting and to verify their instructions, and high levels of personal data protection
- *High transparency and consumer information* on the security standards associated with the available services, so as to ensure consumers make informed decisions
- *Limitations* on deposit or transfer amounts

From Basic to Evolving

In line with the proportionality principle, CDD rules should be progressive or tiered. In countries where a national ID system or equivalent identification measures are not in place, stringent customer-identification requirements may be disproportionate to the risk of the transactions. CDD rules should thus vary with the amount of information the system needs from customers, the documentation customers must submit to verify that information (for example, proof of identity, birth certificates, evidence of residence), and how these documents are in turn verified (for example, through face-to-face meetings, cross-referencing to other databases, verification by third parties).

Risks are mitigated by the systems' ability to identify customers appropriately and to record transactions digitally. This reduces the anonymity that is associated with the use of cash and allows the tracking of individual transactions and the monitoring of their number, frequency, and scale. The Financial Action Task Force allows countries to adopt risk-based (proportional) regulations to ensure that measures to prevent or mitigate money laundering and the financing of terrorism are commensurate with the risks identified (FATF 2012). A risk-based regulation, for instance, would provide for the application of lighter identification and verification requirements for lower-risk services (for example, small-value e-money transfers and payments) and more stringent requirements for riskier ones.[77] Several countries define at least one differentiated type of account with lower CDD requirements. In several cases, e-money accounts also bear different limitations for transaction amount. Ceilings are low for basic accounts, higher for mid-range accounts, and much higher for full-CDD accounts, which are used mostly by agents and merchants who handle larger amounts of cash and higher transaction

volumes than the regular clientele. Digital ID systems (discussed in box 6) and KYC registries can play a highly critical role in a DPS environment and may enable countries to leap directly from the basic to innovating DPS ecosystem level.[78]

Today, payment-system overseers worldwide are paying more and more attention to the need to protect payment systems and services from cyber risk and the risk of fraud. Preparedness to deal with these types of risk and to ensure resilience to their materialization should be integral to the risk-management responsibilities of each and every stakeholder of the NPS. In particular, the adoption of international standards and best practices should be recommended for the correct use of digital devices for DPS.[79] The Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions have issued important guidance in this critical area (CPMI-IOSCO 2016; CPMI 2018), and the International Telecommunication Union has examined the security vulnerabilities of the stakeholders involved within the DPS ecosystem and recommended specific measures (ITU 2017e). DPS overseers, as well as all relevant policy authorities, should consider incorporating these guidance and recommendations in their requirements and expectations for DPS providers.[80]

From Evolving to Innovating

Higher security and integrity-protection modalities should be implemented for more sophisticated DPS ecosystems. The related strategies should outline the DPS' future state of cyber resilience, in terms of maturity and/or risk, with short- and long-term perspectives, and PSP risk managers should continuously improve and adapt the existing cyber resilience strategy and policy framework as the desired maturity level and/or risk landscape change. Providers should be required to establish the appropriate structures, processes, and relationships with the key stakeholders in the DPS ecosystem to enhance the ecosystem's cyber resilience continuously and proactively. In addition, authorities at the national level should set up a computer emergency response team to apply real-world solutions to various cybersecurity problems. Response teams may be government contractors or employees of a major corporation. They are not just "antivirus team" tools; new kinds of cyberattacks are constantly surfacing, and security professionals need to stay ahead of these problems. They need to look at end-point security as well as security for data in use and at rest; they need to do testing and simulations to anticipate security problems before they arise; and they also need to do quick damage control on problems that have not been anticipated. The work of a computer emergency response team encompasses a wide spectrum of security activities aimed at preventing and minimizing cyberattacks from wherever they originate, and it involves doing work to reduce occurrences of these problems in the future.

Regarding fraud-risk management, centralized solutions may bear important advantages. Global payment-system operators such as the international card networks and global e-money services such as Paypal have active fraud reporting, monitoring, and mitigation programs in place. These also exist in some domestic payment systems. However, given the wide variety of payment services operating in countries in the innovating category, a holistic program and system for fraud management is needed. Here, the initiative of the Reserve Bank of India is illustrative. In 2019, the bank decided to set up a

Central Payment Fraud Registry with a view to tracking frauds related to DPS. When the registry is deployed and operational, payment-system participants will be given access to the registry for nearly real-time fraud monitoring, and the aggregated fraud data will be published to educate customers about emerging risks. Currently, banks report all banking frauds to the reserve bank's Central Fraud Monitoring Cell . The planned registry may extend the platform to all PSPs. It will help the reserve bank to collate periodic data for customer awareness.

Strengthening Competition

Competition is necessary for sound and dynamic DPS ecosystems to develop.[81] DPS typically disrupt long-standing business models in the financial sector and may harm the revenue of banks. For this reason, banks may have an incentive to refuse interoperability with the new non-bank entrants. Similarly, financial institutions may resort to bundling and cross-subsidization between platforms and services in order to favor their digital payment units over their competitors. Such actions may be deemed to be anticompetitive whenever they are carried out by operators with market power and lead to the exclusion of as-efficient competitors. In addition, financial institutions may enter into collusive agreements to delay the transition to DPS (see, for example, the French Competition Authority case on bank fees collusion), or a payment association may refuse{-EDIT OK?-} to accept new members (for example, the European Commission's decision on Visa's decision to refuse Morgan Stanley membership of{-in?-} Visa Europe, Groupement des Cartes Bancaires).

Competition policy in a country should reflect the country's level of DPS ecosystem development. While such indicators of market power as large market share, high margins, and high market concentration provide useful first-order indications of the market structure and the relative importance of the various firms operating in the market, they are insufficient to determine whether a DPS provider has market power and the incentives to abuse it. In fact, such indicators can be misleading in digital markets, since competition between a few players can be intense and current market leaders can be effectively displaced in a short period of time. In digital markets, a key indicator of market power is usually the power to exclude, which is not necessarily associated with higher market shares or higher profits, and competition authorities should focus on anticompetitive conduct and its (likely or actual) effects and should not infer market-power concerns from market structure. The critical element for determining the existence of market power pertains to the actual contestability of the market in light of the relevant market conditions and market dynamics. For market expansion or entry to be likely, it must be sufficiently profitable for the competitor or entrant, taking into account factors such as the barriers to expansion or entry, the likely reactions of the allegedly dominant undertaking and other competitors, and the risks and costs of failure. Policies for basic ecosystems should focus on market entry, while market conduct and market structure should be at the core of competition policy for the higher levels and for the country's accompanying transition from the evolving to the innovating level.

From Basic to Evolving

The public authorities should facilitate competition by opening the DPS market to new entries. Aside from differences involving income, sector characteristics, and management capabilities, differences in the use of DPS country-wide may be due to regulatory or market impediments.[82] Possible impediments are market distortions and protections that allow incumbent firms to maintain profits without threats from more innovative entrants. Preventing non-banks from entering the DPS market and permitting them to do so only indirectly (through banks) weaken market competition and hinder innovation as well as use of DPS.[83] On the other hand, new businesses may successfully enter the market because of underregulation. In this case, while allowing underregulated entrants into the market may benefit consumers through more convenience and lower prices, new players (for instance, platforms) may establish themselves in the market, capture the market owing to the scale and network economies inherent in the nature of their business, and use their extra profits to buy out competitors or to preclude them from developing rival services. The authorities should thus remove barriers to market entry by establishing a consistent legal and policy framework for providers of tried and tested payment services (such as mobile money), possibly introducing the category of "Payment Service Providers" and establishing authorization and oversight requirements to allow legal persons (including also non-banks) to supply payment services across the national jurisdiction.

Large-volume recurrent payment streams should be leveraged to advance the diffusion of DPS across the economy and attract entry of new providers. These streams can be leveraged to drive investment in core retail payment infrastructure as well as in distribution channels and the development of new payment products and services. Several large-volume payment streams are characterized by the fact that one party to the transactions (for example, the national treasury, an employer, or a provider of a utility) has significant control over the terms and features of the payment product that offer the potential to drive financial inclusion. Examples are government payment programs, utility payments, public transit payment programs, employer payroll programs, and remittances (both cross-border and domestic). The Committee on Payments and Market Infrastructures and World Bank Group examined the role of all these payment streams as catalytic pillars to advance the adoption and usage of DPS in the context of financial inclusion (2016) and recently reconsidered them in light of fintech developments (2020). They will not be repeated here. It is important to note that, in order to realize the potential of such payment streams, the other measures to encourage and facilitate the use of DPS are needed.

Enlisting a large merchant base that accepts DPS is critical to expand competition in the DPS ecosystem. Especially with a view to including the underserved, it is fundamental to ensure acceptance from small merchants who are located in and cater to low-income communities. The Principles on Identification for Sustainable Development (Principles 2017) looks specifically at the issue of digitizing merchant payments in developing countries and identifies six key obstacles to deepening these payments: (i) an inadequate value proposition for merchants, including product design that does

not adequately encourage them to migrate from cash to digital payments; (ii) weak product and stakeholder economics in traditional card models; (iii) insufficient aggregate customer demand, needed to reach the "tipping point" that drives demand and supply toward a digital payments ecosystem; (iv) an inconsistent technological infrastructure and regulatory environment to support digital payments; (v) ineffective distribution models to serve hard-to-reach merchants in areas with limited economic capillarity; and (vi) difficulty in formalizing enterprises and the reluctance of merchants to pay full taxes on sales.

The authorities should protect and support market competition. Dominant players may adopt exclusive arrangements with agents, impose price and access conditions that might restrict use by competitors of necessary network services (for example, for telecommunication), resist regulatory decisions to introduce interoperability between services of different providers, and exercise control over customer data. As a consequence, start-ups are left with tiny niche markets (if they are left with any at all).[84] One should consider, however, that a tendency toward market concentration is an inherent feature of business models that are based on networks with strong supply-side (scale and scope) and demand-side (network) externalities, and in particular those that are characterized by a two-sided market structure (box 8). Also, "collective dominance" may occur in markets with a limited number of firms where no single one of them holds significant market power, but all of them, together, may possess (and exercise) dominance collectively. Under collective dominance, firms must be able to reach a coordinated position; they must be able to monitor each other; deviating from the coordination must be perceived as costly; and other firms and customers must not be able to undermine coordination. The major policy concerns are to make sure that the market remains contestable by potential new entrants and that the market-dominating firm does not abuse its power to prevent new entries and to extract extra surplus from consumers. Therefore, subject to the considerations discussed in the context of the payments infrastructure, the authorities should prohibit exclusivity arrangements that could lock in the market power acquired by any individual provider, require interoperability in system design, and foster interoperability to the extent feasible, as discussed.

The public authorities should protect the DPS market from anticompetitive practices and ensure that PSPs conduct their business in ways that are consistent with competition principles. In particular, the authorities should prevent the abuse of dominant positions and the exclusion of competitors for reasons other than the merit of their products. As discussed, suppliers of network services—such as MNOs—may face two potentially conflicting incentives: to increase the wholesale supply of their upstream telecommunication network services to PSPs (including mobile-money PSPs), and to protect their market position from (actual and potential) rivals in the downstream retail (including the same mobile-money PSPs). However, there is a feedback loop from the retail mobile-money services market into the retail mobile telecommunication market. Where an MNO has a dominant position in the mobile-money services market, it has a strong incentive to channel demand to its own transfer and payment services. By maintaining and strengthening its position in the mobile-money market,

BOX 8 COMPETITION IN TWO-SIDED MARKETS

Buyers of video-game consoles want platforms on which to play games, and game developers pick platforms that are or will be popular among gamers. Cardholders value credit or debit cards only to the extent that these are accepted by the merchants they patronize. Affiliated merchants benefit from a widespread diffusion of cards among consumers. More generally, many, if not most, markets with network externalities are characterized by the presence of two distinct sides whose ultimate benefit stems from interacting through a common platform.

To succeed, platform owners or sponsors in industries such as software, portals and media, payment systems, and the Internet, must "get both sides of the market on board."

Under multisidedness, platforms must choose not only a price structure but also a price level for their service. For example, video game platforms such as Sony, Sega, and Nintendo make money from game developers through per-unit royalties on games and fixed fees for development kits, and they treat the gamers side as a loss source. On the other hand, operating system platforms for the PC and handheld devices have adopted the opposite business model and aim to make money from consumers. The choice of a business model is key to the success of a platform and receives much corporate attention.

Conventional wisdom about business models points to some fundamental logic related to prices and surpluses on both sides of the market. From both positive and normative viewpoints, two-sided markets differ from the textbook treatment of multiproduct oligopoly or monopoly. The interaction between the two sides gives rise to strong complementarities, but the corresponding externalities are not internalized by end users, unlike in the multiproduct literature (where the same consumer buys the razor and the razor blade).

Some critical questions raised by two-sided markets are specific to the existence of competition between platforms. In a number of markets, a fraction of end users on one or both sides connect to several platforms. (Using Internet terminology, they are "multi-home.") For example, many merchants accept both American Express and Visa, and many consumers have both Amex and Visa cards in their pockets. Many consumers have the Internet Explorer and the Netscape browsers installed on their PC, and a number of Web sites are configured optimally for both browsers. Readers may subscribe to multiple newspapers, business-to-business exchange members may buy or sell their wares on several exchanges, and real estate sellers and buyers may use the services of multiple real estate agencies. Competitive prices on one market then depend on the extent of multi-homing on the other side of the market. For example, when Visa reduces the charge paid by merchants, merchants are tempted to turn down the more costly Amex card as long as a large fraction of Amex customers also own a Visa card. More generally, multi-homing on one side intensifies price competition on the other side, as platforms use low prices in an attempt to steer end users on the other side toward an exclusive relationship.

The two-sided market structure—including its inherent economies of scale and scope, multi-homing, and stickiness—engenders concentration in the core infrastructure. Yet, if played right, it may bring more competition in the market. This can be achieved only by balancing the level of cooperation and competition within the system hosting it, and access to service and service efficiency become vitally important. In the market for DPS, one of the critical factors is access to financial infrastructures. In this regard, private-sector providers can mitigate transaction costs by cooperating when establishing and operating financial infrastructures, taking advantage of economies of scale, scope, and network externalities. The study of the DPS market structure is critical to understand how economies of scale, scope, and network externalities may affect

BOX 8, continued

the behavior of users and providers. DPS providers compete directly in the provision of payment instruments and services to end users, but they also cooperate in shared-payment networks. However, coordination failures do always not make it possible to cooperate, thereby introducing inefficiencies or duplications. On the other hand, cooperation may result in collusive behavior by players that have a dominant position in the payments infrastructure. The focal point is the trade-off between cooperation and competition, and the potential impact of oversight and regulatory intervention. In this context, the appropriate role of oversight and regulation, or more generally, the need for government intervention to maximize social welfare, has been debated. It thus becomes important to identify the policy issues and regulatory implications stemming from cooperation versus competition in DPS.

Source: Rochet and Tirole (2003); World Bank (2008).

the firm also strengthens its position in the mobile telecommunication market, since subscribers need to access the latter to obtain the former. Thus, MNOs can use their market power over communications channels to leverage network effects and use them to prevent competitors from gaining traction in the downstream mobile-money services market. Strategies include refusing to provide data services to competitors, offering prices that squeeze competitors' margins and make their business commercially unviable, and discriminating in pricing, quality of service, and other terms. The harm can extend into all areas of the mobile financial-services market. For instance, if banks offer their services across mobile networks in competition (rather than in partnership) with the MNOs, the development of mobile savings and lending services may be impeded by the latter. The authorities should intervene when MNOs refuse to supply services to competing PSPs.[85]

From Evolving to Innovating

In addition to the above policies, in more sophisticated DPS markets, competition policies should guard against the abusive behavior of large multiproduct companies and, in general, all entities having significant market power, through a combination of ex ante regulation and ex post enforcement. Anticompetitive behavior may originate from the ability of such entities to establish connections between their different products with a view to exploiting their dominance in one market to extend it to the DPS market and to discriminate against competitors. For example, they may bundle their products and condition the sale of one product on the use of the DPS they provide, or they may use their position as gatekeeper to other markets to give preferential treatment to their own DPS and discriminate against those from third parties. Such practices should call for drastic measures, such as the introduction of neutrality requirements that ensure non-discrimination in the way that digital platforms treat third-party products and services. A strong and credible competition-policy stance from the authorities should induce large technology companies to adopt more open competition standards in the expansion of their DPS business. Box 9 discusses the importance of ex ante regulation in digital markets, and box 10 illustrates two examples of competition policy in the DPS market.

BOX 9 EX ANTE REGULATION IN DIGITAL MARKETS

In digital markets, the main competition issue is usually the power to exclude, which is not necessarily associated with higher market share or profits. The use of traditional structural indicators of market power can be misleading for these markets, since competition between a few players can be intense and displace market leaders relatively quickly.

Certain characteristics of digital markets (for example, network and scale effects, lack of multi-homing and lock-in effects), coupled with the conduct of the companies operating in those markets, can create a threat to competition. Risks to competition arise in markets where some players acquire a gatekeeper position. These are typically firms with large bases of loyal customers that can determine how and whether third parties can access these customers.

Significant consumer harm can derive from gatekeeper platforms' attempts to gain revenue from their platform users (for example, users of a smartphone platform) at the expense of third-party firms offering complementary services (for example, developers of apps for that smartphone platform). Such harm is more likely to arise as the platform business (for example, the sale of smartphones) slows.

Several jurisdictions (for instance, an overwhelming number of Organisation for Economic Co-operation and Development members, including those in the European Union) have adopted institutional architectures that establish one or more specialist ex ante regulatory agencies and a distinct ex post competition enforcement authority. The former agencies seek to promote market contestability by facilitating market entry (ex ante), thus seeking to identify problems beforehand and shape stakeholder behavior and responses through regulatory intervention, while the latter intervenes once competition rules have been breached by a market player (ex post).

However, the need for better policy tools is being felt. The alleged market abuse by gatekeeper platforms has become a pressing concern in regulatory and competition debates, and several such gatekeeper platforms have recently been accused of privileging their products and services over competitors or directly excluding competitors' services. The European Commission, for instance, is consulting on creating an ex ante regulatory framework for gatekeeper platforms and establishing a new competition tool to make it easier to intervene where there are structural market problems, and the United Kingdom is developing its plans for a Digital Markets Unit that would, among other things, set a code of competitive conduct for strategically important firms. With specific reference to the financial sector, following the financial crisis, new models emerged with respect to the role

FIGURE 13: Comparison between Ex Ante and Ex Post Regulation[86]

	Sector-specific regulation	Competition authority
Primary objective	Orderly growth of sector resulting in consumer welfare	Consumer welfare and curbing monopoly power
Focus	Specific sectors of economy	Entire market economy
Mode	*Ex ante*	*Ex post*
Method	Tells businesses 'what to do' and 'how to price products'	Tells businesses 'what not to do'
Issues handled	Regulating access, prives, reducing barriers to entry, changing market structure, facilitation competition	Affecting conduct of entities maintaining competition

BOX 9, continued

of competition for services provision. For example, in 2015 the UK Financial Conduct Authority gained concurrent powers for enforcement of competition policy. Supervisors in other jurisdictions have also been granted competition-related powers or have introduced new methods of cooperation with competition authorities.

A report from the GSM Association (GSMA 2016a) assesses how governments and regulatory authorities can update competition and regulatory frameworks to realize the full potential of the digital economy. Its policy recommendations are grouped into four areas: i) market definition and assessment of market power; (ii) adoption of a total welfare standard in place of the consumer welfare standard; (iii) the balance between ex ante and ex post regulation; and (iv) institutional arrangements. In particular, the report recommends that governments review the thresholds established for ex ante regulation to ensure that the expected gains from regulation are balanced against the risks to investment and innovation. Alexiadis and da Silva Pereira Neto (2019) provide an extensive analysis of the policy choices and trends related to institutional design of competition law and regulatory enforcement, and point to the different architectures that can be adopted to reconcile and bring together tools used to regulate the behavior of undertakings ex ante and to sanction eventual abuses ex post.

Source: Rochet and Tirole (2003); World Bank (2008).

Markets can be competitive and deliver beneficial outcomes even when they are dominated by large players, provided that the following conditions obtain:

- New providers may enter the market easily (including by taking over incumbents) and offer innovative products that the community values.
- Existing smaller incumbents may expand and capture market share from their rivals.
- Consumers may conveniently switch to alternative products or providers.

Thus, while the limits imposed by regulation on market entry and expansion should be minimal and risk based, effective scrutiny of the adverse use of market power by participants should be integral to the responsibilities of the public authorities. Also, the power of consumer choice should be strengthened, enabling consumers to switch more readily between DPS providers—for instance, by giving them the right to have their financial data transferred from one provider to another, such as under open banking and APIs.

In more sophisticated DPS markets, large-scale data collection and analysis may bear potential for anticompetitive effects. *As noted by the GSM Association (2016b),* **t***he widespread collection, storage, and processing of data in some cases may lead to barriers to entry for new rivals. While data per se need not raise competition issues, such issues may arise when dominant firms use user data to create cross-platform synergies that allow them to become gatekeepers to essential inputs.*

BOX 10 COMPETITION POLICY AND THE DPS MARKET: THE EXAMPLES OF CHINA AND THE UNITED KINGDOM

China

In 2016 alone, China saw $9 trillion in mobile payments—in contrast to a comparably small $112 billion worth of mobile payments in the United States. The use of mobile payment systems such as Alipay and WeChat Pay are widespread in China; users range from beggars to lenders to criminals. Previously, the mobile payments landscape was largely untouched and unregulated by the Chinese government because of its relative insignificance in the Chinese economy. However, with the explosive growth in mobile-payment transactions, the People's Bank of China (PBOC) implemented a new mobile-payment regulation on June 30, 2018, requiring all mobile payments to be cleared through the bank. Consequently, transactions completed over mobile-payment networks can no longer be settled directly through the mobile-payment platform provider and must be sent to the centralized clearing house for settlement. This means that invaluable, previously proprietary consumer data collected by mobile-payment platform providers such as Alipay and WeChat Pay is now sent to the centralized clearing house, where other mobile-payment platform providers and banks have access to it. The bank's stated reasoning for implementing this regulation is to curb money laundering and fraud.

United Kingdom

In 2016, the Payment Systems Regulator reviewed the ownership and competitiveness of infrastructure that supports the three major payment systems in the United Kingdom: Bacs, Faster Payments Service, and LINK (PSR 2016).[87] The review found that (i) there is no effective competition for the provision of payments infrastructure for the three main interbank payment systems (Bacs, FPS, and LINK); (ii) the lack of competitive procurement exercises by the operators is a barrier to entry that prevents potential providers from competing; (iii) the UK payment systems' bespoke messaging standards act as a barrier to entry for new infrastructure providers into the UK market; and (iv) because of the joint control that the four largest shareholder PSPs exercise over both the operators and VocaLink, the current ownership and governance arrangements are likely to reduce the level of competition. The review proposed a package of measures, including the following:

- Competitive procurement exercises: There are a number of ways this could be implemented, ranging from issuing guidance to requiring operators to follow a prescribed procurement process.
- Enhanced interoperability, including a common international messaging standard, for Bacs and FPS. (A common international messaging standard for LINK might have unintended consequences and more limited benefits compared to Bacs and FPS.)
- Divestment by the four largest VocaLink shareholder PSPs of their interest in VocaLink, noting that the acquisition of VocaLink by Mastercard could by itself address the issues identified as causing a restriction of competition.

The authorities should prevent (where possible) or penalize excessive and discriminatory pricing practices. Charges for the use of the telecommunication network for mobile financial services may vary considerably.[88] Increasingly, network operators enter into partnership agreements with financial institutions to provide DPS. In such cases, they may have an incentive to offer their partners better pricing and more convenient access conditions than they offer to competing PSPs. This might include, for instance, removing usage-based charges. Such zero-rate pricing represents a competitive advantage over competing providers, where the latter or their customers have to pay based on usage. Network operators may discriminate in favor of their partners as well as aggregators that bring to them larger volumes of business than they themselves are able to generate. Such discriminatory practices should be considered unlawful under either competition or telecommunication laws, since they distort or harm competition. *The monitoring of pricing practices can be complemented by giving consumers more information. Better price information and more disclosure on the costs of various DPS can help consumers identify uncompetitive products, start formal complaints, or both.*

Furthermore, the authorities should intervene when network operators impose a "margin squeeze." A margin squeeze occurs when a network operator charges a rival PSP a wholesale price for its network service, typically USSD (Unstructured Supplementary Service Data), that does not leave the rival enough of a margin between the wholesale price and retail price in the market for payments for the rival to make the supply of such downstream retail services commercially viable. Margin squeeze is commonly recognized as an anticompetitive strategy for raising the rivals' costs, whether to gain a competitive advantage or to exclude the rivals outright from the market. In many countries, there are signs of margin squeezes being imposed by dominant MNOs on their competitors.[89]

There are multiple theories about how competition-based precepts should be applied to the digital economy.[90] In practice, competition-related jurisdiction and powers are generally founded on national competition laws and sectoral regulations. *Competition law may empower both sectoral regulators and competition authorities. In fact, n*ot all countries have a competition law or competition authority, and sectoral regulators are often given mandates that allow them to intervene within their sector over specific competition issues. Sectoral regulations usually contain provisions allowing the authority to intervene prior to the occurrence of issues, so as to ensure a fair and level playing field. In the case of competition law, on the other hand, the authority may intervene only after or when an issue has occurred—typically, an infringement of rules (box 11). Sector regulators may also be granted powers to act ex post (for example, to enforce competition rules ex post) similarly to competition authorities, as is the case in the telecoms sector.[91]

Addressing anticompetitive behavior requires intervention under the competition law (if there is one), the telecommunication law or relevant sectoral law, or both. The liberalization of network industries has had a decisive influence on competition law and policy in several jurisdictions. Its evolution cannot be understood without considering the progressive opening to competition of sectors such as energy, postal services, and telecom-

BOX 11 COMPETITION-RELATED REGULATORY RESPONSES

COMPETITION AUTHORITIES

Competition authorities have tools that are clearly delimited by legislation and are executed within specific competition mandates. The tools are usually in the form of ex post intervention and include the following:

Investigations: A regulator or competition authority may be able to initiate an investigation of anticompetitive behavior. This may be done either on its own accord or based on industry complaints. Such an investigation usually takes the form of a market review and analysis and may include the sending of questionnaires to all of the market participants and economic modeling. If, after the review, a competition issue is indeed substantiated, the regulator may formally charge the relevant entity, whose final recourse then is to appeal through the judiciary or a specific competition appeals body. Sanctions for a finding of a breach of competition law may include fines, structural remedies, behavioral remedies, and, possibly, criminal penalties, such as prison sentences.

Injunctions/interdicts: The ability of the authority to request injunctions/interdicts to stop temporarily potential anticompetitive behavior before it can complete any necessary market review if the harm is immediate and irreversible.

Merger reviews: The ability of the authority to review merger and acquisition operations to ensure that they do not raise any competition issues after the merger and, in many jurisdictions, the ability to render such operations conditional on approval (possibly with conditions, including structural or behavioral remedies).

Sectoral Regulators

To date, sectoral regulators with competition-related competencies employ a variety of methods (that usually do not apply to competition authorities) to approach or resolve competition issues. These include the following:

Regulatory forbearance: Here the responsible regulators—aware of a competition issue and having the power to intervene—allow the market to come to a solution.

Use of moral suasion: The responsible regulators use a light-touch and coordinated approach to persuade the market participants to come to a satisfactory resolution to their competition dispute(s) on their own and at the risk of the regulators stepping in to mandate a solution if they do not.

Intervention: If the parties are unable or unwilling to resolve their disputes, the responsible regulators may intervene. The intervention, for example, may relate to pricing and/or access rights by competitors to a specific service. The regulators may also intervene unilaterally, based on policy precepts, without a competition issue necessarily being raised with them.

Blunt instrument: The regulators may employ a blunt-instrument approach. For instance, they may break into two independent entities—one for operating the infrastructure, say, the other for providing services—an entity that has been shown to have abused its vertically integrated market power. The newly independent infrastructure entity would then have to provide access to all market participants at fair, reasonable, and non-discriminatory terms, while the newly independent services entity would be in the same position as all other market participants and would now have to obtain its access from the new infrastructure entity at market-related prices.

Source: ITU (2017a).

munications. Competition in these sectors is peculiar in that it often revolves around a segment that tends toward monopoly. Cases against incumbent operators make up a significant fraction of the enforcement activity of competition authorities. From a qualitative standpoint, it is apparent that, as a result of the liberalization process, some substantive issues have acquired a level of prominence that they did not have in preceding decades and that they would not otherwise have had. In the financial-services sector, and in the retail-payments market in particular, exclusion of competitors can support and embed a vicious circle of network effects that raise the risk of entrenching dominance deeply. In some countries, regulators are beginning to react. Box 12 reports an illustrative example of competition policy in Kenya's DPS sector.

To ensure effective implementation of competition policy, the law should clearly define which authority (authorities) are responsible for DPS competition issues and grant it (them) sufficient powers and autonomy, including the power to enforce rules and deci-

BOX 12 COMPETITION IN DIGITAL PAYMENTS: THE CASE OF KENYATRIES

The Competition Authority of Kenya is a state corporation and was established by the Competition Act No. 12 of 2010. It is mandated to promote and safeguard competition in the national economy by effectively enforcing competition law and rules economy-wide, opening markets by advocating for the removal of anticompetitive sector regulation and protecting consumers and suppliers. The authority has intervened in a number of sector cases. With specific regard to the market for digital payments, the shapes below report the identified issues, the policy actions taken, and the results achieved.

PROBLEM

- Safaricom was found to have abused its dominant market position by entering into exclusive contracts with MPESA agents.
- Safaricom was found to have abused its dominant market position by practicing excessive pricing and price non-transparency on transactions going through its network
- Safaricom was found to have abused its dominant market position to impede account-to-account interoperability.

ACTION

- Safaricom, in a settlement with the Competition Authority of Kenya, agreed to open up MPESA agents to all market players.
- Safaricom, in a settlement with the authority, agreed to lower service charges and to inform PSPs of transaction prices via real-time notification after initiation but before completion.

In April 2018, interoperability was launched. The three relevant authorities (Communication Authority, Competition Authority, and the Central Bank of Kenya) cooperate to facilitate interoperability

RESULT

- Agent profitability increased by 10 percent; consumer savings increased by $33.2 billion; bank networks expanded from 5 percent in 2013 to 15 percent in 2014.
- Consumers can switch between services as they can compare costs; service charges decreased from one-half to one-tenth of the original charge.
- Transaction costs dropped; competing PSPs' business increased.

Source: Kariuki (2019).

sions. An existing regulator or a new agency should be given a clear mandate to take the lead on matters related to competition in the DPS market and to address gaps in the regulatory architecture related to the lack of effective competition in the DPS market. Given that DPS involve cross-industry products, it is not always clearly defined who the competent authority should be for competition policy issues. This uncertainty could create jurisdictional conflicts between authorities. In addition, regulatory requirements for DPS (for example, for access and participation) may have implications for market competition, while the protection and promotion of competition may require the regulatory intervention of agencies other than the competition authority (for example, rules on information transparency and disclosure).[92] Thus, in those jurisdictions where a competition authority coexists with sector regulators that share competition responsibilities, all agencies should coordinate their acts, and mutual cooperation agreements should be established to ensure that regulations and policy measures leave no gaps and that overlapping responsibilities do not hamper the action of each agency. Enforcement of competition rules in DPS provision can be attributed to the competition agency solely or jointly with the central bank and the telecommunications regulator. Where there is no established competition authority, sector-specific regulators should be empowered and encouraged to lead and to define a coordinated way forward on competition issues and to streamline enforcement. Finally, all agencies involved in competition policy should be granted sufficient autonomy, protecting them from the risk of political interference and pressure from the lobbying interest of private-sector stakeholders.

Given the complex nature of DPS, competition authorities or sector-specific regulators should have specific expertise relating to DPS and related issues. One reason why competition problems often go unidentified, or are identified only at a late stage, is the lack of institutional expertise on DPS issues. Regulators may lack knowledge in economic-competition analysis due to insufficient skills or sectoral experience. To ensure timely identification of competition problems, the allocation of adequate (financial and human) resources should be ensured, thus allowing the authority to handle DPS matters satisfactorily.

A national financial-stability committee should implement a process of review before individual financial authorities put in place regulatory interventions that may have a material impact on competition in a product or service market. A member of this public body should be designated to take up the role of assessing planned interventions and to establish possible consequences for competition in financial markets. The assessment of competition impacts should be discussed collegially, and, if necessary, amendments to regulatory actions should be considered to reduce the effects on competition. Competition analyses and minutes of all committee meetings should be made public in a timely manner.

A final consideration is in order. Financial regulation is not incompatible with the promotion of competition in financial services in general and in the provision of DPS in particular. In this regard, effective competition can be seen as a secondary objective of financial regulation, in addition to promoting the safety and soundness of the firms regulated (Bank of England 2020). Hence, competition should develop within a strong

ex ante regulatory framework in which financial firms are prevented from excessive risk-taking (especially for systemic reasons). In light of the interplay between prudential regulation and competition policy, it is critical that regulators and competition authorities liaise and coordinate their actions in order to prevent the adoption of decisions that fail to take into consideration both the competition and regulatory objectives.[93]

Protecting, Informing, and Educating the Consumer

A sound and dynamic DPS ecosystem requires consumer confidence. This, in turn, requires that consumers perceive the DPS ecosystem both to be reliable and to provide consumers with sufficient protection of their rights as customers. Issues such as the inability to initiate or complete transactions (due, for instance, to network downtime or cumbersome processes) act as deterrents to successful usage and acceptance of DPS by customers. Similarly, uncertainty about PSPs or other third parties' use of the information and data concerning the customers may weaken consumer trust in DPS and discourage or limit their use. Regulators should ensure that the relevant networks, platforms, and other technical elements for DPS delivery are in place and function properly. In addition, regulators should require PSPs to adopt quality-of-service standards and risk-management practices that are appropriate to the nature of the DPS delivered, and they should monitor the PSPs' performance and compliance with rules on an ongoing basis.[94,95] Finally, regulators should establish PSP liability rules for losses suffered by consumers caused by such events as fraud, agent misconduct, or quality-of-service issues (for example, network downtime).

From Basic to Evolving

Clear rules for transaction disputes should be instituted for all payment methods. *The rules should be transparent for both payers and payees and take into account typical profiles of users of particular payment instruments and access channels.* Regulators should require PSPs to set up easy-to-understand, efficient, and free-of-charge claim-redressal procedures, effective dispute-resolution mechanisms, and efficient customer-assistance services (for example, hotlines and communication channels). *Also, robust mechanisms for escalating consumer complaints should be put in place. It should be easy for customers to lodge complaints about disputes that remain unresolved by their PSPs. It would be beneficial if the platform facilitating dispute resolution worked across different payment instruments, channels, and types of financial institutions and offered channels that take into account different genders, cultural backgrounds, and levels of financial literacy.*

A sound and dynamic DPS ecosystem requires transparency and customer information. When customers face significant impediments or costs in their search for alternative providers, or where there are only a small number of providers, the providers may be able to set service prices and quality without regard to competition or consumer pressure. On the other hand, transparent and simple pricing makes it easier for customers to compare services, thus creating competitive pressure on providers to improve prices, quality, and varieties and to innovate processes and products. Where there is competition but market information is unavailable (for instance, about service charges), consumers may have difficulty comparing the offers available from different providers.[96] Regulators should

establish standard definitions for costs and fees and require disclosure to be in line with these standard definitions, so to ensure consistency across providers. Regulators should also require disclosure of fees prior to the completion of a transaction, and customers should have the option to cancel transactions after disclosure.

From Evolving to Innovating

A sound and dynamic DPS ecosystem must protect customer data. Breaches of privacy and particularly data security may result in identity theft, harm to financial records, fraud, and other risks. Poor people tend to be more vulnerable than rich ones. A range of privacy and data-protection issues need to be addressed in DPS markets. This requires regulatory provisions to obtain effective consent (including through opt-in permissions for use of customer data). Rules on data sharing, data-use liability, and third-party liability, and privacy and marketing rules, place greater responsibility in the hands of consumers.[97] Yet an incomplete understanding of data issues and their associated risks, and an appetite to access the services, are likely to reduce the protection afforded by effective consent systems. Regulators may thus impose some basic protective measures (including, for instance, disclosure rules on how customer data should be collected by PSPs or third parties, and on how they{-customers or data?-} should be treated and used) and require the industry to adopt at least minimum (internationally accepted) standards.

A sound and dynamic DPS ecosystem needs financially educated customers. Even if DPS are in high demand, customers may lack the general knowledge and financial literacy necessary to protect their rights as consumers. Shortcomings in financial literacy pose challenges for the policy authorities and service providers seeking to expand the use of new payment services, especially to excluded and underserved people.[98] The evolution of DPS is a source of complexity for users who may have little experience or no experience at all with digital devices, whether mobile or online. Policy authorities and market players must cooperate to facilitate user access to, and awareness of, digital financial tools, making sure customers are given simple instructions on how to use new tools and services and information on what to do when dealing with instantaneous, non-face-to-face transactions causes problems.[99] A broader and deeper financial knowledge helps raise the awareness of customers, merchants, and businesses (especially small ones) of the benefits, costs, and risks of using DPS and supports a better use of DPS.

Guidance has been developed by the G20 to strengthen digital and financial literacy and awareness (OECD 2018). *This guidance is aimed at identifying and promoting effective initiatives in light of the unique characteristics, advantages, and risks of DFS and channels, to support their evaluation and dissemination and to promote a responsible and beneficial development of digitalization by building trust and confidence in the acquisition and use of DFS by the financially excluded (box 13). Other key actions to enhance DPS literacy and awareness include, among other things, the following:*

- Encourage the development of practical, accessible, and digitally focused financial-literacy and awareness programs (particularly for underserved and vulnerable groups) to help consumers understand the features, benefits, risks, and costs of DPS.

BOX 13 POLICY ACTION CHECKLIST FOR THE DESIGN AND IMPLEMENTATION OF EFFECTIVE FINANCIAL-EDUCATION INITIATIVES ON DFS

The *G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy* offers actionable steps in the design and implementation of financial-education initiatives on DFS to strengthen the digital financial literacy of consumers and entrepreneurs (OECD 2018). This box summarizes the five key areas that are addressed in more detail in the guidance note.

Depending on national circumstances and on the policy actions that might already have been taken by public authorities in the context of a national strategy for financial education and/or inclusion and consumer protection measures, policy makers should make sure the following steps are considered when implementing digital financial-literacy initiatives. This list does not imply that they should be implemented in a particular order. The first step—data collection—should be considered a priority, however.

- Develop a national diagnosis of the impact of digital finance on individuals and entrepreneurs (including potentially vulnerable groups) and collect key indicators on the supply and demand side of DFS.
- Ensure coordination between public authorities and private and not-for-profit stakeholders involved in financial literacy and innovation in a way that avoids conflicts of interest.
  - Map actors providing DFS and assess the online platforms and tools used to understand the message conveyed and possible risks.
  - Involve private and not-for-profit stakeholders in the design and implementation of digital financial-literacy initiatives.
  - Develop and enforce codes of conduct/good practices to limit and manage potential conflicts of interest.
- Support the development of a national core-competency framework on digital financial literacy of consumers and entrepreneurs to accomplish the following:
  - Build trust and promote beneficial use of DFS and related technological innovation
  - Protect consumers and small businesses from vulnerability to digital crime and misuse/mis-selling
  - Empower consumers to counter new types of exclusion due to the potential misuse of data sources, including data analytics and digital profiling
  - Support consumers at risk of overreliance on easy access to online sources of credit

Accordingly, map existing provision of financial education and verify whether this covers financial education for DFS as described in this framework, and, if not, promote its inclusion and/or develop tailored initiatives.

- Support effective delivery of financial education through digital and traditional means and address the needs of target audiences through tailored approaches.
  - Exploit the advantages of digital delivery: easier access to financial education, messages tailored to the audience, and support for money-management skills while reinforcing core competencies.
  - Design an appropriate delivery mix depending on the audience, taking into account the relevance of traditional delivery for priority groups and vulnerable populations.
- Facilitate and disseminate evaluation of financial-education programs addressing DFS.
  - Encourage the use of a standardized evaluation toolkit at the national level, to better understand impact and suggest positive change.
  - Share the results at the national and international level.

Source: OECD (2018).

- Encourage informed choices by consumers through the development of tools allowing them to compare similar DPS (such as price-comparison websites).
- Harness the DPS industry (if necessary, with public support) to develop financial-literacy and digital-literacy programs that build knowledge, understanding, and confidence in the use of DPS.
- Raise awareness among small businesses of the advantages of processing payments and fund transfers digitally.

2. DRIVERS

The drivers of the strategic approach consist of actions that the public authorities and relevant stakeholders should undertake to set in motion the development of a sound and dynamic DPS ecosystem. The drivers ensure that the appropriate *building blocks of the strategy are in place and work together effectively and* include (a) overseeing the DPS ecosystem effectively, (b) inducing cooperation between the DPS overseer and other relevant public authorities, (c) engaging stakeholders in the policy dialogue on DPS issues, and (d) acting strategically and with discipline. The drivers for a specific level of DPS ecosystem are (e) leveraging large-volume, recurrent payment streams, and (f) broadening merchant acceptance of DPS.

Ensuring Effective Oversight

Strong oversight is key for building up sound and dynamic DPS ecosystems.[100] In this regard, the overseer (in cooperation with other regulators, as necessary) should seek to create the conditions to facilitate the development of DPS both by promoting market competition and innovation and by preserving public trust in the systems and instruments used for transferring funds—trust that the methods of payment will work, trust that the value being transacted will remain throughout the transactions, trust that the systems will not be abused, and trust that, in case of errors, there are steps to take. Oversight seeks to ensure that DPS provision is safe, efficient, and inclusive; robust and resilient to risks; constantly available; and evolving based on the changing needs of the economy.

The overseer of the DPS ecosystem may play several roles. It adopts rules, standards, and policy guidelines for the good conduct of PSPs, and it monitors and ensures PSP compliance with such rules, standards, and guidelines. It acts as regulator and supervisor of DPS provision. The overseer makes sure that PSPs, as well as all entities operating in the NPS space, manage carefully the risks that arise from their payments activity and that such risks do not become systemic. The overseer also encourages cooperation from NPS stakeholders and coordinates their action when this is necessary to increase the efficiency and safety of payment infrastructures. (See below.) An important part of the oversight role is to catalyze the modernization of the NPS; in that context, the overseer promotes use of DPS and the protection of DPS user rights. More broadly, the overseer contributes to creating a conducive environment for the development of a sound and dynamic DPS ecosystem and provides services that are necessary to support it. In so

doing, the overseer should be neutral as to the technologies evolving in the market (provided their associated risks are well managed) and should not promote or favor any particular technical solutions. Selecting technical solutions should remain a responsibility of the market.

The specifics for oversight policy are discussed elsewhere.[101] Here, it is important to highlight two fundamental elements. First, the overseer should be given enough authority and resources to conduct effective oversight and to use all instruments necessary to this end. It is especially critical that the overseer be empowered to access all the needed information and to induce all required changes in the DPS ecosystem, consistent with its oversight objectives.[102] It is as critical that the overseer avails itself of tools and methodologies to oversee DPS providers and digital payment instruments, ensuring that they manage risks effectively (both the risks that they face from operating in the NPS space and those that they pose to other NPS entities as well as to their customers), and providers of services that are critical to DPS provision (for example, technology solutions).[103] Exercising authority effectively is essential for the overseer to gain authoritativeness with DPS stakeholders.

The second element is the overseer's ability to use its authority and authoritativeness to balance cooperation and competition in the market for DPS. A complex tapestry of intertwined factors at the level of governance, access, and pricing have a bearing on the deployment of competitive, efficient, and scalable DPS. Examples of factors that could hamper DPS development include, among others, the preponderant role that incumbents may play and the potential to abuse market-dominant positions; the fact that rules and conventions may underpin distorted charging practices; the lack of appropriate transparency arrangements as regards pricing and policies to be applied; and the rise of coordination failures affecting the rate of payments innovation. Providers of DPS should thus be induced to compete on services and to cooperate on infrastructures. This requires the overseer to engage relevant NPS stakeholders in undertaking collective action aimed at addressing issues of common concern (see below) and to prompt DPS providers to compete vigorously and fairly in trying to win over consumer preferences (World Bank 2008). The adoption of risk-based rules and oversight tools, and the capacity to hold an ongoing policy dialogue with stakeholders, are necessary ingredients for the overseer to strike a sound balance between these two objectives.

Improving statistics should be integral to overseeing a sector as highly innovative as DPS provision. Reliable statistics are critical for identifying and designing appropriate oversight responses to payment innovation, and initiatives are needed to improve the statistical reporting on PSPs, including information on their activities, risks, and financial resources. While the evolution of payment-service provision by non-bank PSPs is particularly important for DPS overseers, information on PSPs and their activity is also needed for areas such as cybersecurity, competition policy, and consumer protection. Hence, there is a need to monitor new trends, and this requires harmonized statistical definitions across regulatory institutions.[104]

DPS overseers should also improve their data-collection processes. Automated processes will maximize the efficiency and effectiveness of information management and will minimize errors and data losses. Solutions are available today that can improve the scope, procedures, and techniques of payment-system oversight and financial supervision. Examples include those that move away from using historical data and toward accessing data in real time at the institutions' IT systems directly, dynamic compliance,[105] the use of APIs by overseers, and machine learning. The latter can help overseers analyze digital data, mitigate challenges in data collection and analytics, and even predict the behavior of different institutions. Overseers should also consider adopting information-management approaches that will allow for enhanced data quality and availability (by shifting from aggregated to granular data, increasing the scope of data, and reducing the time to report) and will automate the collection and analysis of unstructured data. New solutions include the "input approach," whereby the institution uploads the standardized granular data automatically into a central data warehouse at or accessed directly by the overseer;[106] the "pull approach," in which the supervisor extracts (pulls) raw granular data from the institution's IT systems; and the so-called regulatory reporting utilities, consisting of a common interface between the overseer and reporting institutions that can provide several services, such as compiling regulatory requirements, translating the related dictionary/taxonomy into computer codes, and storing data.

Taking a CooperativeApproach

Developing a sound and dynamic DPS ecosystem entails cooperation at multiple levels. Cooperation is required between the DPS overseer and other relevant authorities, [107] and between the overseer and DPS stakeholders. The coexistence of diverse legal institutions within the DPS space and the variety of policy dimensions involved in the provision of DPS (for example, consumer protection, market conduct, market integrity, data integrity and information security, financial inclusion, financial stability, payment-system modernization, economic and financial-sector development, and so on) cross the interest and mandate of several public authorities. It is imperative that all relevant authorities cooperate with each other to foster efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates with respect to DPS. Such cooperation needs to be effective in normal circumstances and should be adequately flexible to facilitate effective communication, consultation, or coordination, as appropriate, during periods of market stress, crisis situations, and the potential recovery, wind-down, or resolution of infrastructures or PSPs. Cooperation may also be important at the regional and international level. Where domestic payment systems are linked with non-domestic infrastructures, or where plans are in place for regional integration, cooperative arrangements should be established between the relevant regulatory, supervisory, and oversight authorities in the region.

Cooperation may take different forms.[108] The form, degree of formalization, and intensity of cooperation should promote the efficiency and effectiveness of the cooperation and be appropriate to the nature and scope of each authority's responsibility for the supervision or oversight of the DPS. Cooperative arrangements should be managed to ensure the efficiency and effectiveness of the cooperation with respect to the number of authorities participating in such arrangements. Where cooperative arrangements are

appropriate, at least one authority should accept responsibility for establishing efficient and effective cooperation among all relevant authorities.[109] Authorities should commit to full and mutual collaboration and establish effective lines of communication and exchange of information. Protocols can be agreed to between them to define the terms of their mutual cooperation, determine the flows of information, and identify the operational modalities of the cooperative relationship, with the primary objective being facilitating and speeding up the adoption of suitable action by those who are best placed to intervene in critical situations. The DPS overseer and other relevant authorities could sign a memorandum of understanding in which all signatories agree to cooperate in carrying out their tasks with due respect to their mutual responsibilities. The memorandum would describe the purpose of the agreement; lay out the scope, procedures, terms, and conditions for information sharing, policy consultation, and coordination; and provide a list of contact points to which information or requests for information and assistance would be directed under the memorandum of understanding.[110]

An ongoing and structured policy dialogue should take place with the DPS stakeholders. The DPS overseer should promote an active policy dialogue with all DPS stakeholders, including also users.[111] In market environments characterized by knowledge-intensive and fast-changing production and delivery processes, as well as by sophisticated products and complex institutions, communication between market players and public regulators and legislators is a necessary multi-way learning opportunity. The dialogue should consist of consultations on specific issues, regular and ad hoc discussions on issues of common interest to stakeholders, and joint work on technical issues. The policy dialogue would enable the overseer to align stakeholder expectations around common goals and offer a channel for the overseer to communicate its policy orientation, solicit stakeholder views and feedback, and share knowledge on DPS issues.

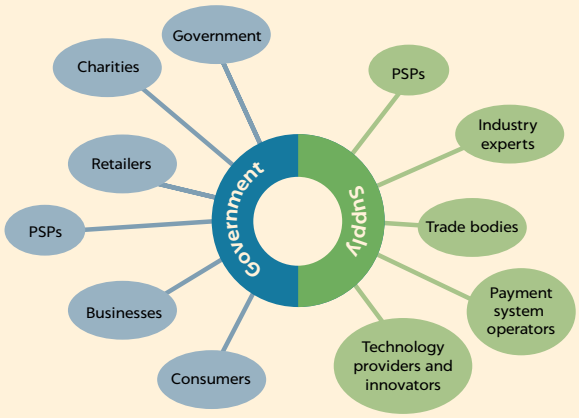
The policy dialogue should take place in a dedicated forum such as a national payments council or payments association. The forum should be established under the leadership of the DPS overseer and provide an opportunity for the overseer to engage with the stakeholders, to discuss and agree with them on initiatives to strengthen the NPS and the DPS ecosystem and to induce collaborative efforts for the design and implementation of the strategy choices. The role and remit of the forum should be defined by the overseer and reflected in specific terms of reference. The composition of the forum should be as inclusive as possible, and its participants should represent the broadest range of existing stakeholders (box 14).

The DPS overseer should act as secretariat of the forum. It should prepare the forum's agenda and organize its meetings, liaise with the members and all parties involved in the forum's work, and ensure that proper follow-up action is taken on forum deliberations. The forum should be run transparently. The secretariat should engage with consumers, small users, and other groups that are not well represented in the payments industry. To ensure better engagement, these individuals and groups should be given opportunities to interact with the forum through various channels of communication, such as website updates, meetings, roundtables, and events. The forum should be supported by a number of working groups. The working groups should comprise

BOX 14 PAYMENTS FORUM: AN EXAMPLE FROM THE UNITED KINGDOM

The UK Payments Strategy Forum was announced by the Payment system Regulator (PSR) in 2015. The forum leads a process to identify, prioritize, and help to deliver initiatives where it is necessary for the payments industry to work together to promote collaborative innovation. The forum's central focus is to make payment systems work better for those that use them. Currently, the forum consists of a chair, who is independent from industry, and 22 members. The membership includes user representatives and PSPs. The Bank of England, the Prudential Regulatory Authority, the Financial Conduct Authority, and the PSR are observers. The PSR also provides the secretariat to the forum.

The forum was established to provide an opportunity for payment service users to engage with and influence strategic initiatives that the forum undertakes. The forum's role and remit was defined by a multistakeholder working group that helped to develop both the wider policy and its terms of reference. Its composition was designed to be as inclusive and effective as possible. The members represent the broadest range of stakeholders, from banks to technology providers, consumer representatives, and businesses.



The chair has a strong background in consumer affairs, ensuring that a strong consumer and user focus remains at the heart of the forum's work. The forum meets at least six times in its first year. More meetings may be scheduled as required. It is guided by the Payments Community (see below) and supported by a number of working groups.

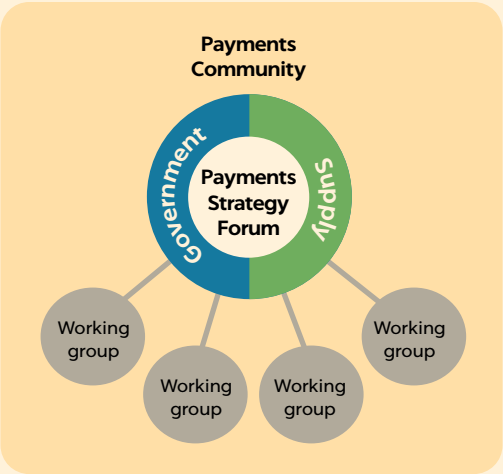
The working groups are the engine room of the forum and cover four areas: end user needs, access, security, and innovation. They inform the work of the forum and help it achieve its goals. They have a clear remit to analyze issues, produce conceptual solutions, and prioritize action according to those that are expected to deliver the greatest net benefit to users. The working groups meet regularly and comprise individuals with expertise from different areas within the payments industry, including service user representatives. They have been resourced by a range of stakeholders from the payments industry and beyond who have seconded staff, made available workspace, and provided funding for independent evaluation of their work.

The PSR established the Payments Community to influence the work program of the forum. The Payments Community is open to everyone with an interest in payment systems, regardless of whether they are forum members.

Source: Payment Strategy Forum.

BOX 14, continued

The community provides a flexible way for all interested individuals or organizations to engage in and shape the forum's work. The secretariat has and will continue to engage with the consumer movement, small users, and other groups that have not traditionally been well represented in the payments industry. To ensure that the community has the opportunity to engage in the forum's work, various channels of communication are used, such as website updates, meetings, roundtables, and events.



Source: Rochet and Tirole (2003); World Bank (2008).

individuals with expertise from different areas within the payments industry, including service user representatives. The working groups should have a clear remit to analyze the issues, produce conceptual solutions, and prioritize actions according to those that are expected to deliver the largest benefits to the payments business community.

The overseer should be committed to advancing DPS initiatives through leadership and action. It should act as leader, convener, and catalyst, as appropriate, and commit its resources to supporting these initiatives. The overseer should also actively monitor and communicate publicly the progress achieved, seek feedback from stakeholders, and adjust the strategies in response to actual developments. Beyond inputs garnered through the forum, the overseer should continue to seek input from stakeholders on key issues through live events, surveys, and engagement with industry groups, and it should open online consultation on its website.

Acting Strategically and with Discipline

The authorities should ensure that all related and concurrent strategies are mutually consistent and coordinated. Where a country is undertaking multiple reforms—such as, for instance, in the areas of digital economy, financial-sector development, payment-system modernization, transition to e-government, and financial inclusion—individual strategies should be designed and implemented in ways that are mutually consistent and maximize their synergies. This will be most critical in the case of DPS and DFS development strategies, not only because DPS are the essential conduit to safe and efficient DFS but also because DPS are increasingly embedded into DFS provision (for example, a PSP also providing big data services, or a bigtech company providing its e-commerce platform customers with payment services). As discussed below in subsection IV.C.3, an integrated approach would be especially relevant for the MENA region.

A successful transition to a sound and dynamic DPS ecosystem requires strategic and disciplined actions. The DPS overseer should adopt an operational strategy for developing the national DPS ecosystem that would combine the building blocks and drivers discussed above, so as to translate the strategy into concrete actions to be taken according to a plan, or road map, by identified parties and within given deadlines. The overseer, in cooperation with the stakeholders, should then implement the strategy and monitor its implementation systematically, verifying whether the planned actions are being taken according to the plan, assessing the outcomes, and taking corrective actions if necessary.

Acting strategically requires careful stocktaking at the outset of the strategic process and close monitoring during strategy implementation.

- **STOCKTAKING, POSSIBLY SUPPORTED BY BENCHMARKING, IS NECESSARY FOR STRATEGY PREPARATION, AS THE POLICY MAKERS AND STAKEHOLDERS NEED TO HAVE A CLEAR PICTURE OF THE DPS ECOSYSTEM AS IT STANDS BEFORE TAKING ACTION.** A comprehensive stocktaking should reflect a full description of the existing structure of the ecosystem and incorporate a gap analysis that identifies the missing components, the vulnerabilities that the strategy should address through appropriate policy actions, and the impediments to DPS development that need to be removed. Benchmarking the ecosystem against select (qualitative and quantitative) indicators would help to understand how the ecosystem compares internationally and what could realistically be achieved through a strategy aimed to modernize or reform it. Stocktaking and benchmarking, therefore, are essential steps to determine policy objectives and priority actions.
- **MONITORING STRATEGY IMPLEMENTATION IS ESSENTIAL TO ASSESS PROGRESS.** Monitoring requires the use of a comprehensive and robust data- and information-management system and should build upon the information and indicators used for stocktaking and benchmarking, with a view to assessing the impact of strategy implementation against the goals set, identifying obstacles to implementation, and providing insights about the efficiency, effectiveness, and impact of the reforms and policy programs deployed. Tracking progress could be supported by establishing an online data portal and by publishing regular reports to provide publicly available data on the adoption and use of DPS. The World Bank has elaborated templates for stocktaking and for assessing progress on the use of digital financial (and payment) services. National authorities implementing the strategic approach developed in this report could adopt the templates as a tool.[112]

The policy authorities have key roles to play to encourage merchant acceptance. Examples of actions range from streamlining CDD requirements for merchants seeking to accept digital payments, to incentivizing merchants through some degree of tax-related accommodations (particularly in the early stages), creating incentives for consumers and merchants to transact electronically (for example, granting tax rebates on digital transactions and simplifying tax procedures), and accepting DPS for government services.[113]

BOX 15 NEW PAYMENT METHODS FOR NEW CUSTOMER EXPERIENCES

Invisible Payments

Invisible or frictionless payments are transforming customers' purchase experience in stores. They make the purchase process "disappear" and are based on apps that enable users to select the specific products they want to consume (so that they are ready to be picked up without waiting in line), to schedule favorite orders that can be ordered and paid for automatically, and to effect purchases without having to ask for the bill or to pay manually. Once the customer picks the merchandise, his or her card is automatically charged. The new method benefits users by saving their time, and it benefits merchants, who no longer have to charge customers manually. To automate payments, users just need to register first in the app and enter their credit card details. The application also offers the possibility to share payments with other users by sending a message directly from the app. Some providers are developing software to digitally verify and authenticate one's personal identity through facial, voice, image, document, or fingerprint recognition.

The software utilizes artificial intelligence and machine-learning algorithms through which the machines learn to identify both the users and products in order to make the correct charge on their card. Invisible payments are a key ingredient of contextual commerce.

Contextual Commerce

Amazon's Alexa allows users to call an Uber, order a pizza from Domino's or Pizza Hut, make shopping lists, and place orders. Pinterest's "buyable pins" let consumers buy products with Apple Pay or stored credit card information at the moment that they show intent, without ever leaving the platform. Instagram users can tap the photo for tags as they normally do, but instead of the brand handle, they see product information (such as price, description, and additional photos) and a "Shop Now" button. Uber customers, on the other hand, can securely store their payment information in the app, and their cards are automatically charged once the rider's destination has been reached, taking the friction out of paying and tipping completely. These are just some of the many instances of contextual commerce.

Contextual commerce is a solution to consumers' "want it now" mentality, which that has evolved so rapidly everywhere in recent years. It means meeting consumers where and when they have the most interest and intent to purchase, with the easiest checkout experience as possible (thus, reducing the sales cycle significantly). Contextual commerce aims to facilitate transactions within a customer's current environment (or context). It allows businesses to integrate buying opportunities into everyday activities, and instead of redirecting consumers to an external website, it eliminates a number of steps, delays, and abandonment opportunities on the way to smooth checkouts within platforms.

The DPS industry may also play an important role in addressing some of the challenges. In particular, where small merchants are not willing to employ (costly) standard systems that accept cards, the industry might offer affordable alternative solutions. Examples include low-cost applications that allow small merchants to accept a number of different payment options without having to purchase new POS terminals and through which merchants can receive payments initiated via a cell phone, tablet, or laptop and credited to their accounts in real time and at no charge to the merchant (within a limit); web-based platforms (accessible via Android, desktop, SMS, and USSD)[114] that enable small and medium enterprises to accept, process, and manage multiple mobile-money payments; solutions whereby suppliers partner with PSPs to bring payment services to retailers, such as installing card-accepting machines in small convenience stores; QR code–based payments; and new methods of frictionless payments that facilitate consumer experience and enhance merchant services (box 15).[115]

3. ADDRESSING THE MENA REGION'S CRITICALITIES

The strategy for developing DPS can also help MENA countries to address (directly or indirectly) some their major criticalities: the gender divide, limited competition in the banking sector, youth unemployment, and the large informal economy. Sound and dynamic DPS ecosystems would assist MENA countries in their efforts to improve conditions of access to finance for their people. Reducing the cost and improving the convenience of using DPS, simplifying the requirements for using DPS, and, most of all, strengthening public trust in the DPS ecosystem (including also its institutions and instruments) would go a long way toward addressing the factors that people in the MENA region consider as major obstacles to accessing finance (and discussed in section III).

Sound and dynamic DPS ecosystems are also a necessary precondition for providing safe and efficient DFS. Adopting an integrated approach to digital payment and financial services will be critical, as the MENA region's economic development strategy rests crucially on the promotion of the digital economy and, therefore, requires accessible and reliable DFS. The integrated approach will be even more critical for the MENA region, as it will be instrumental to address the region's identified criticalities: gender discrimination, limited competition in the banking sector, and youth unemployment. {-and the large informal economy?-}

Gender Issues[116]

Governments in the MENA region should consider the gender divide in DPS with a sense of priority. Disseminating the use of DPS and DFS among women by itself will not solve the gender divide in the MENA region in many areas, but it would contribute to the solution by expanding the set of choices and opportunities available to women, introduce positive change in women's economic habits and practices, and eventually influence the social culture as a result. A number of factors—some of them already discussed—may play a critical role as enablers to improve women's access to and usage of DPS. The general point that should be emphasized here is the need for policy makers to form a strategic vision of gender issues and to take on the enablers with coordinated

action that is commensurate to the evolution of the national DPS ecosystem; simply focusing on one enabler at a time will not be enough. Some of the enablers discussed below would also help bring women into the formal economy, thus contributing to addressing another of the MENA region's criticalities discussed below. Finally, it should be borne in mind that DPS would contribute to women's welfare and facilitate their everyday life independently of their employment status, since women (like all men) have normal payment needs whether they work or not, and those should be met by every NPS as conveniently as possible.

Non-banks should be allowed to issue e-money. Licensing non-banks to issue e-money and agent-based models would make it possible for development of products and services that are better suited to women. Women could be helped greatly if DPS were set up to make routine non-discretionary expenses such school fees and utility bills.[117]

PSPs should be allowed to use a wide range of third-party agents to facilitate customers' access to, and use of, DPS. This would create employment opportunities for women to serve as agents and bring greater financial inclusion. Women agents can benefit PSPs, as they have strong potential to boost the providers' performance (IFC 2018b) and would attract more female clients due to social norms and safety concerns that women may have about interacting with male agents.[118] To expand the number of women in agent networks, development practitioners should focus on building the business case for women agents, starting by understanding key capital and training constraints faced by the types of businesses women are likely to own in many developing countries, such as hair salons and food stalls. National public authorities should develop regulations that balance safety and inclusion when determining who is eligible to become an agent.

CDD policies should be proportional and risk based. People with low or no incomes, especially women, often lack access to an official ID document. Traditional CDD requirements that do not consider these constraints deeply affect whether women are able to access formal financial services.[119] Regulations that allow for simplified CDD in lower-risk scenarios and recognize the types of ID documents that women typically have should help to bring more women into the financial system.

A strong commitment to customer protection can boost women's trust in DPS providers. Women often feel sidelined and discriminated against by formal financial institutions, and data protection is also becoming a key factor shaping their DPS access and use. Moving forward, it will be important to obtain more insights on effective data privacy and protection approaches that contribute to responsible financial inclusion of women.

Revitalizing Competition in Banking and Finance

New payment and financial digital technologies may open up the financial sector in the MENA region—which tends to be static—to new providers, thus creating a new competitive environment. For instance, the use of new sources of customer-payment and financial data in the analysis of credit risk, or for the supply of automated

financial and advisory services, may trigger competitive effects that can bring further advantages to current providers (if they are able to exploit the new business opportunities) or may allow new players to get—via alternative ways—information that is relevant to compete in the DPS and DFS markets. Digital platforms and marketplaces offer a vivid example of this: Online communications reduce transaction costs between agents who are geographically dispersed (the search for counterparts, the negotiation and monitoring of contracts, and so forth), and this allows for the emergence of platforms that put borrowers and lenders in contact with each other and facilitate their transactions through trust mechanisms that reduce information asymmetries. Digital channels also tend to improve the comparability of the products and services offered by different providers and reduce the costs incurred by consumers of switching from one provider to another. Also, by specializing in specific payments and services, fintechs unbundle the banking-sector value chain. Within this new environment, banks and other new players become competitors within individual elements of the value chain and work together in other areas, such as when fintechs offer new solutions to banks or when banks incorporate third-party products and services within the value proposition they offer to their customers. In recent years, another kind of player has entered the financial sector: large technology companies (bigtechs) with consolidated positions in other digital markets such as Amazon, Facebook, and Apple in the United States and Europe and Alibaba and Tencent in China. Like the fintechs, these companies also offer specific payment and financial services, unbundled from the banks' value chain. A common aspect of the strategies employed by bigtechs is building around their customers a DPS and DFS ecosystem including social media, e-commerce, search engines, operating systems, app stores, and the like, all of which are mutually interconnected. All this can greatly revitalize competition within the banking and financial sector.

Providing Payment Services to Youth

Digital payment and financial services can help youth in the MENA region to access resources to build their job skills and manage their income sources. Youth in the region are three times as likely to be unemployed as adults; rural youth face more limited employment prospects; and young people often enter adulthood without access to financial services due to barriers such as limiting social norms, legal and regulatory restrictions, and perceptions of un-employed youth as low-value and high-risk customers. As discussed, gender, too, plays an important role in youth livelihood choices, employment, and wages, as young women have even fewer opportunities than their male counterparts to be employed and financially included. DPS and DFS can help families manage major expenses linked to educational and training opportunities essential to building young people's skills and increasing their employability, productivity, and income, and digital platforms can open unprecedented opportunities for youth to access education, training, goods, markets, and financial and non-financial services by changing the delivery of information. DPS can facilitate young people's access to the digital economy—for instance, by enabling them to receive payments from both domestic and foreign buyers of services rendered online or to acquire goods and services from domestic and international markets that allow them to participate in the digital economy (for example, online courses, cloud computing, and so forth). Anderson, Hopkins, and Valenzuela (2019) suggest policy actions that can be taken to exploit

the power of DFS in this ambit. While this area transcends the remit of this report, this discussion offers an opportunity to reiterate the importance for MENA countries of creating sound and dynamic DPS ecosystems as conduits to safe and efficient DFS.

Narrowing the Informal Economy

Sound and dynamic DPS ecosystems may assist MENA countries in their efforts to reduce the informal economy. While the MENA region does not suffer from economic informality issues any more than other emerging market and developing economies regions do (see section III), the phenomenon occurs to an extent that requires action. Many financially excluded individuals and firms are found in the informal economy, and the digitalization of payment services offers an important means of addressing the eligibility and affordability barriers to formal financial inclusion faced by informal individuals and firms. In particular, digitalization can facilitate identity verification, promote DPS provision, and improve the information environment. However, in order to fulfill its potential, digitalization requires that attention be given to financial consumer protection and financial education—two of the strategic building blocks discussed above. The G20's *Policy Guide* presents a set of key policies that support the delivery of interventions to facilitate financial inclusion of individuals and firms operating in the informal economy (GPFI 2018). The guide focuses on four key areas that can ease eligibility and affordability barriers (appendix F).

4. DPS FOR EMERGENCIES

The outbreak in 2019 of the COVID-19 pandemic has prompted important considerations in many countries worldwide on the use of DPS for emergency situations. Crises such as COVID-19 may place extreme strains on payment and settlement systems both because of the operational risk that the health aspects of the crises pose and financial risks that arise from the impact on the health of the financial sector and the whole economy. In response to the crisis, countries took restrictive measures to stop the virus from spreading. These restrictions inevitably had impacts on short- and longer-term economic activity as well as the incomes of all—notably the most vulnerable. While these preventive measures were taken, authorities considered issuing measures to ease the burden of these restrictions on the economy as a whole, as well as on individuals and firms.

The use of DPS would be critical in such crisis circumstances. Events like the COVID-19 pandemic may impair payment services directly and indirectly by their impact on the availability of the payment systems. The direct impact on payment services is on those that require manual intervention and/or physical presence/interaction, including cash. In contrast, DPS may experience little or no impact (although they could be indirectly impacted by operational problems affecting the underlying payment and settlement systems). DPS can help the economy and society at large to endure situations where physical contacts among individuals are restricted or not permitted yet money flows have to be secured to the extent possible through the economy and across the whole country, possibly allowing each and every (adult) resident to access and use funds as and when necessary. In the specific case of crises relating to contagious diseases, DPS

can support the public by reducing the risk of infection from handling cash. DPS provision can facilitate a smoother functioning of the remaining economy. It can mitigate the economic impact of the crisis on the most exposed, including informal workers, and by facilitating money flows, it can support economic activity (production and exchange) that otherwise would be impossible.

The strategic approach places special attention on extending the use, availability, and continuity of DPS, so residents of crisis-hit countries can access essential services and make/receive payments.[120] The approach comprises policy measures and actions that national financial authorities can implement immediately and over a longer time horizon—in coordination with NPS stakeholders as necessary—to facilitate access to essential services via the provision of DPS. Given the scope of this report, the approach focuses on DPS only. Elsewhere, the World Bank has elaborated a broader strategy covering all relevant aspects of payment-system response in the context of COVID-19.[121,122]

In order to make the use of essential services possible at a time when economic activity in the country is restricted, critical DPS need to be provided. These payment services facilitate the delivery of salaries from employers to employees; pensions to pensioners; government subsidies, in the form of transfers, to households in need, informal workers, and existing beneficiaries of social programs; person-to-person remittances (both domestic and cross-border); bill payments, loan disbursements, and debt/loan repayments; payments for transportation services by users; and payments to merchants.

Providing essential services requires a continuous supply while consumers keep making their payments in exchange for use of these services. This can prove difficult for countries where a large share of the population works in the informal sector, holds seasonal jobs, works in non-essential sectors, and there is a significant loss of jobs and household income. During the COVID-19 pandemic, some countries took measures to postpone the repayment of loans or the payment of utility bills. Some considered providing an expanded program for social cash transfers to those affected the most—for example, the poorest, those who lost their jobs due to closures of non-essential businesses, and informal workers who lack job security and unemployment insurance. Some countries provided support to the SME sector due its relative vulnerability compared to the large corporate sector.

Expected Impacts of Crisis on Access to Essential Services

In all crisis situations where movement of individuals exposes society to greater risk (epidemics are an example), country authorities typically turn to extensive measures aimed at minimizing those movements. Measures include establishing curfews or movement restrictions for certain segments of the population (for example, categories of people who are considered vulnerable or more at risk) or for the population as a whole, with exceptions for the provision of essential services. Such restrictions imply that the provision of most, if not all, essential services is to be done using digital platforms, where feasible. For example, shopping for groceries, medicine, and so on could done remotely; payments could be made in cash upon delivery or digitally. In the specific case of con-

tagious diseases, mitigating the risk of infection would also require that payment be made by means other than cash and checks.

Based on experiences with COVID-19 of payment markets in emerging markets and developing economies across the world, the following impacts on access to essential services can be expected during crisis situations:

- Operational disruptions to payment and settlement systems due to the unavailability of staff due to illness, work-from-home restrictions, or increased risk of cyber threats caused by home-based work and any resulting inability to carry out critical risk-management processes
- Vulnerabilities in the risk-management frameworks of payment and settlement systems that lead to credit and liquidity risks that cascade from one or more participants of a system to other participants and potentially to other payment systems
- Risks to the distribution of or access to cash—for example, as a result of the closure of bank branches and agents due to non-essential business status or location (for example, inside a shopping mall), the closure of agent locations of remittance service providers in the sending countries and hence a sudden stop (or sharp decline) in remittance inflows, and an inability to provide ample liquidity to rural access points or those that are outside major cities (for example, ATMs and agents)
- Concerns about using physical currency notes and coins due to perceptions of their being vehicles for the spread of the virus, leading individuals without access to digital payments to lose the ability to make and receive payments
- Inability to use DPS by a large proportion of the population, owing to financial exclusion (voluntary or involuntary), a lack of financial or digital literacy, a lack of awareness or merchant acceptance (partly due to informality), and perceived or actual high costs.

Policy Responses to Facilitate Access to Essential Services via Provision of DPS

A number of DPS-based policy responses should be considered. These include the quick deployment of DPS solutions tailored to vulnerable and financially excluded populations, awareness raising and the assurance of financial consumer protection, and measures for payment systems and other financial market infrastructures. Box 16 describes the measures taken by the Central Bank of Egypt, and appendix G elaborates on each of these types of measures.

BOX 16 DPS AND COVID-19: THE EXAMPLE OF THE CENTRAL BANK OF EGYPT

On March 20, 2020, the Central Bank of Egypt issued a circular to facilitate easier access to basic transaction accounts by financially excluded people and to encourage the usage of DPS. The circular called for the following steps to be taken:

- Limits on the daily value transacted via mobile wallets were to be increased to LE 30,000 (about $1,900).
- Banks were to issue prepaid NFC (near field communication) cards.
- Banks were to improve the merchant-acceptance landscape by encouraging the use of QR codes and the request-to-pay method.
- Banks were to enroll their customers automatically to Internet banking services (as opposed to requiring a physical signature for enrollment).
- Full electronic KYC: Banks were to use tools available to them to ensure at the time of account opening that the mobile wallet owner owned the line registered to the service—for example, banks were to send the potential customer's ID number (NID) and mobile phone number to Egypt's National Telecommunications Regulatory Authority, which would respond with a confirmation of the match between the NID and mobile phone number. Remote account opening for mobile wallets would be feasible.
  - For existing customers, upon receipt of a mobile wallet request, banks were to check with the MNO to confirm the match between the customer's ID and mobile phone number.
  - For new customers, upon receipt of a remote mobile wallet application along with a photo of the NID sent via a mobile phone, the NID/mobile phone number match would be requested from the National Telecommunications Regulatory Authority as above.
  - As MNOs need to do KYC checks at registration, the introduction of this process will increase the speed of opening mobile wallets by reducing the need for multiple checks and verifications.
- These measures were valid for six months.

On March 22, 2020, the central bank issued a circular to make all domestic money transfers exempt from fees and commissions, aiming to decrease the use of cash. Receipts of international remittances were not included.

Source: Central Bank of Egypt.

REFERENCES

Accenture. 2018. *Payments in the Digital Age: How the Digital Payments Paradigm Is Redefining Banking*.

ACM (Autoriteit Consument en Markt). 2017. *Fintechs in the Payment System: The Risk of Foreclosure*. Netherlands Authority for Consumers and Markets, The Hague, December.

Ahrend, R., J. Arnold, and F. Murtin. 2009. "Prudential Regulation and Competition in Financial Markets," OECD Economics Department Working Papers No. 735. OECD Publishing, Paris.

Alexiadis, P., and C. M. da Silva Pereira Neto. 2019. *Competing Architectures for Regulatory and Competition Law Governance*.

Anderson, J., D. Hopkins, and M. Valenzuela. 2019. *The Role of Financial Services in Youth Education and Employment*. Consultative Group to Assist the Poor, June.

Arcand, J. L., E. Berkes, and U. Panizza. 2015. "Too Much Finance?" Journal of Economic Growth 20: 105–48.

Arezki, R., R. Y. Fan, and H. Nguyen. 2019. Technology Adoption and the Middle-Income Trap: Lessons from the Middle East and East Asia, Policy Research Working Paper 8870. World Bank Group.

Autoridade da Concorrência (Portuguese Competition Authority). 2018. *Technological Innovation and Competition in the Financial Sector in Portugal: Issues Paper* (draft for public consultation). Autoridade da Concorrência, April.

Bank of England. 2020. *Prudential Regulation Authority Annual Report, 1 March 2019 to 29 February 2020*.

BCBS (Basel Committee on Banking Supervision). 2018. *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors.* Bank for International Settlements, Basel, February.

Bill and Melinda Gates Foundation. 2015. *Assessing Risk in Digital Payments: Special Report, Financial Services for the Poor, February 2015*.

Bossone, B. 2008. *Integrating Macroeconomic and Financial Sector Analyses within IMF Surveillance: A Case Study on IMF Governance*, Independent Evaluation Office Background Paper BP/08/11. International Monetary Fund, Washington, DC.

Bossone, B. 2017. "*Electronic Money versus Money: An Assessment of Regulation."* VoxEU, January 25, 2017.

Bourreau, M., and T. Valletti. 2015. "Competition and Interoperability in Mobile Money Platform Markets: What Works and What Doesn't?" *Communications & Strategies* 99 (*3rd* quarter 2015): 11–32.

Bundeskartellamt. 2017. "Bundeskartellamt Has No Objection to Paydirekt's New Payment Function," press release, April 12, 2017.

BusinessTech. 2014. "South Africa Gets First Solar Powered ATMs," *BusinessTech*, November 9, 2014.

Capgemini-BNP Paribas. 2018. *World Payments Report 2018*. Capgemini and BNP Paribas.

Caron, F. 2017. *Enabling Technologies in Financial Market Infrastructures and Payment Services Innovation: An Overseers' Perspective on Opportunities, Risks and Policy*. National Bank of Belgium.

CMA (Competition and Markets Authority). 2016. *Retail Banking Market Investigation: Final Report*. Competition and Markets Authority, August.

Competition Bureau Canada. 2017. *Technology-Led Innovation in the Canadian Financial Services Sector: A Market Study*. Competition Bureau Canada, December.

CPMI (Committee on Payments and Market Infrastructures). 2014. *Non-Banks in Retail Payments*. Bank for International Settlements, Basel, September.

CPMI. 2016. *Fast Payments—Enhancing the Speed and Availability of Retail Payments.* Bank for International Settlements, Basel, November.

CPMI. 2017. *Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework.* Bank for International Settlements, Basel, February.

CPMI. 2018. *Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security*. Bank for International Settlements, Basel, May.

CPMI-IOSCO (International Organization of Securities Commissions). 2016. *Guidance on Cyber Resilience for Financial Market Infrastructures*. Bank for International Settlements, Basel, June.

CPMI-IOSCO. 2019. *Responsibility E: A Compilation of Authorities' Experience with Cooperation*. Bank for International Settlements, Basel, December.

CPMI Markets Committee. 2018. *Central Bank Digital Currencies*. Bank for International Settlements, Basel, March.

CPMI-World Bank Group. 2016. *Payment Aspects of Financial Inclusion*. Bank for International Settlements and World Bank Group, April.

CPMI-World Bank Group. 2020. *Payment Aspects of Financial Inclusion in the Fintech Era.* Bank for International Settlements and World Bank Group, April.

CPSS (Committee on Payment and Settlement Systems). 2005. *Central Bank Oversight of Payment and Settlement Systems*. Bank for International Settlements, Basel, May.

CPSS. 2012. *Innovations in Retail Payments: Report of the Working Group on Innovations in Retail Payments*. Bank for International Settlements, Basel, May.

CPSS-IOSCO. 2012. *Principles for Financial Market Infrastructures*. Bank for International Settlements, Basel, April.

CSJ (Centre for Social Justice). 2016. *The Use of Digital Technologies to Tackle Financial Exclusion: Roundtable Report, 7th July 2016*. Centre for Social Justice, London.

di Castri, S. 2013. *Mobile Money: Enabling Regulatory Solutions*. GSMA, February.

Digital McKinsey. 2016. *Digital Middle East: Transforming the Region into a Leading Digital Economy*. McKinsey & Company, October.

EC (European Commission). 2017. "Antitrust: Commission Confirms Unannounced Inspections Concerning Access to Bank Account Information by Competing Services." MEMO/17/3761, October 6, 2017. http://europa.eu/rapid/press-release_MEMO-17-3761_en.htm.

ECB (European Central Bank). 2018. *Cyber Resilience Oversight Expectations for Financial Market Infrastructures*. European Central Bank, December.

ECN (Economist Corporate Network). 2016. *The Future of Digital Finance*. Economist Corporate Network.

FATF (Financial Action Task Force). 2012. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations.* Financial Action Task Force, February.

Fisher, P., and P. A. Grout. 2017. "Competition and Prudential Regulation," Bank of England Working Paper No. 675. Bank of England.

Flaming, M., C. McKay, and M. Pickens. 2011. *Agent Management Toolkit: Building a Viable Network of Branchless Banking Agents—Technical Guide.* Consultative Group to Assist the Poor.

FSB (Financial Stability Board). 2017. *Financial Stability Implications from Fintech: Supervisory and Regulatory Issues That Merit Authorities' Attention*. FSB, June 27.

FSB. 2019a. *Crypto-Assets: Work Underway, Regulatory Approaches and Potential Gaps.* FSB, May 31.

FSB. 2019b. *Fintech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications. FSB,* February 14.

Gévaudan, C., and D. Lederman. 2020. "Stages of Development of Payment Systems: Leapfrogging across Countries and MENA's Place in the World," Policy Research Working Paper 9104. Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/284091578403310061/Stages-of-Development-of-Payment-Systems-Leapfrogging-across-Countries-and-MENAs-Place-in-the-World.

Göll, E., and J. Zwiers. 2018. *Technological Trends in the MENA Region: The Cases of Digitalization and Information and Communications Technology (ICT)*, MENARA Working Papers No. 23. MENARA, November.

GPFI (Global Partnership for Financial Inclusion). 2016. *G20 High-Level Principles for Digital Financial Inclusion*. GPFI and G20 2016 China.

GPFI. 2018. G20 *Policy Guide: Digitisation and Informality: Harnessing Digital Financial Inclusion for Individuals and MSMEs in the Informal Economy*. Global Partnership for Financial Inclusion and G20 Argentina 2018.

G7 France. 2019. *Chair's Summary: G7 Finance Ministers and Central Bank Governors' Meeting*, Chantilly, July 17–18, 2019.

GSMA. 2015. *Competition Policy in the Digital Age: A Practical Handbook*. GSMA, October.

GSMA. 2016a. *Resetting Competition Policy Frameworks for the Digital Ecosystem.* GSMA, October.

GSMA. 2016b. *Safeguarding Mobile Money: How Providers and Regulators Can Ensure that Customer Funds Are Protected*. GSMA, January.

GSMA. 2017. *State of the Industry Report on Mobile Money: Decade Edition: 2006–2016*. GSMA.

GSMA. 2018. *The Mobile Economy: Middle East and North Africa 2018*. GSMA.{-???-}

Gupta, V. K. 2015. "Competition Issues—Experiences from India," presentation to Telecom Regulatory Authority of India, July 15, 2015, https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/1_2%20Competition%20Issues%20-%20Experiences%20from%20India.pdf.

Helms, K. 2019. "G20 Leaders Issue Declaration on Crypto Assets—A Look at Their Commitments." Bitcoin.com, July 1, 2019.

HelpAge International. 2012. *Electronic Payment for Cash Transfer Programmes: Cutting Costs and Corruption or an Idea ahead of Its Time?*, Pension Watch Briefing No. 8, http://www.cashlearning.org/downloads/Pension-watch-briefing-no-8-FINAL.pdf.

ICA (Icelandic Competition Authority). 2017. "Measures to Spur Competition in the Retail Banking Market—Based on a Settlement with Arion Bank," press release, June 22, 2017.

IFC (International Finance Corporation). 2018a. *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*. International Finance Corporation, March.

IFC. 2018b. *Digital Access: The Future of Financial Inclusion in Africa*. Mastercard Foundation and International Finance Corporation, May.

IFC. 2018c. *The Egyptian Fintech Ecosystem: Accelerating Financial Inclusion*. World Bank Group, October.{-SOURCE UNAVAILABLE VIA GOOGLE-}

ILO (International Labour Organization). 2006. *Freedom of Association: Digest of Decisions and Principles of the Freedom of Association Committee of the Governing Body of the ILO.* 5th ed. International Labour Organization, Geneva.

IMF (International Monetary Fund). 2018. *IMF Policy Paper: The Bali Fintech Agenda*. International Monetary Fund, October.

IMF. 2019. *Financial Inclusion of Small and Medium-Sized Enterprises in the Middle East and Central Asia*, Middle East and Central Asia Departmental Paper No. 19/02. International Monetary Fund.

IMF-World Bank Group. 2019. *Fintech: The Experience So Far.* International Monetary Fund and World Bank Group, May 17.

ITU (International Telecommunication Union). 2016a. *Digital Financial Services: Regulating for Financial Inclusion—An ICT Perspective*. International Telecommunication Union.

ITU. 2016b. *Payment System Oversight and Interoperability*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, November.

ITU. 2016c. *Payment System Oversight and Interoperability: The International Dimension*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, November.

ITU. 2016d. *Regulation in the Digital Financial Services Ecosystem*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, May.

ITU. 2017a. *Competition Aspects of Digital Financial Services,* ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, March 2017.

ITU. 2017b. *Identity and Authentication*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, January.

ITU. 2017c. *Main Recommendations*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, March.

ITU. 2017d. *The Regulator's Perspective on the Right Timing for Inducing Interoperability: Findings of a Survey among Focus Group Members*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, February.

ITU. 2017e. *Security Aspects of Digital Financial Services (DFS)*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, January.

ITU. 2017f. *Technology Evolution and Innovation in Digital Financial Services (DFS)*, ITU-T Focus Group on Digital Financial Services Technical Report. International Telecommunication Union, March.

Jetley, N. 2014. "*Solar ATMs Changing the Face of Banking in India." Tech Edge (blog),* CNBC, *April 1, 2014*.

Kariuki, F. W. 2019. "*Competition Law and Policy in the Digital Era: Need for Change?," roundtable* presentation at United Nations Conference on Trade and Development, Geneva, July 11, 2019.

Klapper, L. 2016. "5 Ways Digital Payments Can Bring Women into the Economy." CGAP blog, Consultative Group to Assist the Poor, January 19, 2016.

Liu, A. 2019. "An Analysis of the PBOC's New Mobile Payment Regulation." *Cato Journal* 39, no. 1 (winter 2019): 87–98.

Maes, S., and K. Kiljanski. 2009. "Competition and the Financial Markets: Financial Sector Conditions and Competition Policy." *Competition Policy Newsletter* no. 1 (2019): 12–16.

McKinsey Global Institute. 2016a. *Digital Europe: Pushing the Frontier, Capturing the Benefits*. McKinsey & Company, June.

McKinsey Global Institute. 2016b. *Digital Finance for All: Powering Inclusive Growth in Emerging Economies*. McKinsey & Company, September.

Mersch, Y. 2018. "*Virtual or Virtueless? The Evolution of Money in the Digital Age,"* lecture at Official Monetary and Financial Institutions Forum, London, February 8, 2018.

OECD (Organisation for Economic Co-operation and Development). 2016. *Big Data: Bringing Competition Policy to the Digital Era*, DAF/COMP(2016)14. OECD, October 27.

OECD. 2017. *Big Data: Bringing Competition Policy to the Digital Era—Executive Summary*, DAF/COMP/M(2016)2/ANN4/FINAL. OECD, April 26.

OECD. 2018. *G20/OECD INFE Policy Guidance: Digitalisation and Financial Literacy*. OECD, G20 Argentina, and GPFI.

OECD/INFE (International Network on Financial Education). 2012. *OECD/INFE High-Level Principles on National Strategies for Financial Education*. OECD, Paris, August.

Principles on Identification for Sustainable Development: Toward the Digital Age, endorsed by African Development Bank, Asian Development Bank, Bill & Melinda Gates Foundation, Center for Global Development, Digital Impact Alliance, ID4Africa, International Organization for Migration, Mastercard, Omidyar Network, Open Identity Exchange UK/Europe, Organization of American States, OSCE Office for Democratic Institutions and Human Rights, Plan International, Secure Identity Alliance, GSMA, UNHCR, the UN Refugee Agency, United Nations Children's Fund, United Nations Development Programme, United Nations Economic Commission for Africa, and World Bank Group. World Bank Group and Center for Global Development, February 2017.

PSR (Payment Systems Regulator). 2015. *A New Regulatory Framework for Payment Systems in the UK*, Policy Statement PSR PS15/1. PSR, United Kingdom, March.

PSR. 2016. *Market Review into the Ownership and Competitiveness of Infrastructure Provision*, Final Report, MR15/2.3. PSR, United Kingdom, July.

PSR. 2018. *Data in the Payments Industry: Responses to Our Discussion Paper DP18/1*. PSR, United Kingdom, June.

Rochet, J.-C., and J. Tirole. 2003. "*Platform Competition in TwoSided Markets." Journal of the European Economic Association 1, no. 4 (June 2003): 990–1029.{-OK?-}*

Rossotto, C. M., and M. F. Badran. 2019. "What Are the Policy Challenges for a Digital Economy in the Arab Region? Role of Data, Broadband and Digital Platforms." *Dubai Policy Review* 1 (January 2019).

Smith, G., I. MacAuslan, S. Butters, and M. Trommé. 2011. *New Technologies in Cash Transfer Programming and Humanitarian Assistance: A Study by Concern Worldwide, Oxford Policy Management (OPM) and the Partnership for Research in International Affairs and Development (PRIAD)*. Cash Learning Partnership.

Toronto Centre. 2018. *Advancing Women's Digital Financial Inclusion.* Toronto Centre, January.

UNDP (United Nations Development Programme). 2016. *Arab Human Development Report 2016: Youth and the Prospects for Human Development in a Changing Reality*.

Vives, X. 2016. *Competition and Stability in Banking: The Role of Regulation and Competition Policy*. Princeton University Press.

World Bank. 2008. *Balancing Cooperation and Competition in Retail Payment Systems: Lessons from Latin America Case Studies*, study coordinated by Mario Guadamillas. World Bank, November.

World Bank. 2012. *From Remittances to M-Payments: Understanding "Alternative" Means of Payment within the Common Framework of Retail Payments System Regulation*. World Bank, October.

World Bank. 2019. "Darkening Prospects: Global Economy to Slow to 2.9 Percent in 2019 as Trade, Investment Weaken," press release, January 8, 2019.

World Bank. 2020a. *Competition in Retail Banking Services in Latin America*. World Bank, Washington, DC, September.

World Bank. 2020b. "Impact on Payment and Settlement Systems—COVID Response Note." World Bank, March 27, 2020. https://pubdocs.worldbank.org/en/569471592328283668/Payment-and-Settlement-Systems-COVID-Response-Note-March-27-2020-FINAL-TCV2.pdf.

World Bank Development Research Group, Better Than Cash Alliance, and Bill and Melinda Gates Foundation. 2014. *The Opportunities of Digitizing Payments: How Digitization of Payments, Transfers, and Remittances Contributes to the G20 Goals of Broad-Based Economic Growth, Financial Inclusion, and Women's Economic Empowerment*. Better Than Cash Alliance, Bill and Melinda Gates Foundation, and World Bank Group. August 28.

World Bank Group. 2016. *World Development Report 2016: Digital Dividends.* World Bank Group, Washington, DC.

World Bank Group. 2017. *Distributed Ledger Technology (DLT) and Blockchain*, Fintech Note No. 1. World Bank Group, Washington, DC.

World Bank Group. 2018a. *Digital Economy for Africa (DE4A): Diagnostic Tool and Guidelines for Task Teams*, Version 1.0, November 9, 2018.

World Bank Group. 2018b. *Toolbox for Assessing Digital Finance Development in World Bank Member Countries*, May 2018.

World Bank-World Economic Forum. 2016. *Innovation in Electronic Payment Adoption: The Case of Small Retailers*. World Bank and World Economic Forum, June.

Wrede, P. 2018. "InsureTech for Development." *Private Sector Development Blog*, World Bank, July, 12, 2018, https://blogs.worldbank.org/psd/insuretech-development.

Zhu, X., S. Asimakopoulos, and J. Kim. 2020. "Financial Development and Innovation-Led Growth: Is Too Much Finance Better?" *Journal of International Money and Finance* 100 (February 2020), article 102083.

ANNEX 1

MENA FINANCIAL INCLUSION FOR YOUTH AND WOMEN

Innovation in the area of retail payments is relentless. In a stylized fashion, four subsequent ways of innovation can be distinguished in the retail payments business (figure A1), starting from ***(i) the digitization of bank accounts,*** allowing account holders to mobilize and access their funds electronically via telephone banking in the 1980s and Internet banking in the 1990s, to ***(ii) the delinking of payments from bank accounts*** through the introduction of the prepaid concept, whereby value can be stored in special-purpose accounts (prepaid accounts) and accessed and transacted through digital devices and channels, starting with mobile banking at the turn of the century, to ***(iii) the delinking of the initiation of payments from the maintenance of accounts,*** *so* that third-party PSPs may provide payment-initiation services to customers holding accounts with other financial institutions through initiatives such as open banking via APIs and tokenization, and finally to ***(iv) the delinking of accounts altogether from payments,*** which allows agents to effect electronic fund transfers without having to hold an account with a financial institution—this is the world of crypto-assets and their subset of stablecoins.

These waves of innovation are accompanied by process changes that allow, among other things, for faster payments, which make it possible for money to be transferred from the payer to the payee almost immediately; distributed ledgers of transactions or contracts, which can be maintained in decentralized form across different locations and people, thereby eliminating the need for a central authority to keep a check against manipulation (see below) and also introducing "programmability of money" through smart contracts; the integration of accounts and/or payments with digital ID information; and the use of QR codes.

The expansion of landline and mobile broadband networks and the generalized adoption of smart devices have led to the appearance of new distribution and customer-service channels—e-banking websites first, followed by mobile and online banking apps. Thanks to these developments, payments innovation is radically transforming the user engagement and business models, allowing for continuous interactions between customers and their providers and the embedding of automated payment functionalities into the contexts where customers may need to execute purchases or to send/receive money as they interact socially or commercially. Thus, consumers who are now

FIGURE A1: Innovation in the Business of Payments

4 Waves	Changes in processing	Changes in user engagement and business model
1. Introduction of digital access to bank accounts	Faster payments	Integration with day-to-day interactions
2. Creation of prepaid concept and entry of non-banks	DLT	Invisible payments
3. Delinking of initiation of payment from maintenance of account	Integration with ID	Big Data and Analytics
4. Delinking of account from payment	QR codes	

used to immediacy, ubiquity, and simplicity in digital services (such as social media and e-commerce) have readily taken to these new channels for their day-to-day operations, especially the younger generations.

Advancements in technology disrupt the market for retail payment services; traditional payment methods, channels, and interfaces are fast becoming obsolete. The demand for processing payments faster and in "real time" is rooted in the "anytime, anywhere" expectations of new-age consumers and complemented by the availability of mobile devices, next-generation non-physical interfaces, and a host of new network infrastructure services, as well as by the regulatory push for developing fast and frictionless payment services. The drive from regulation in this area has lately become even more important, not just to support market innovation but to keep innovation from happening in ways that hurt the public interest in the absence of appropriate rules and risk-management provisions. An example is the case of cryptocurrencies operating in totally unregulated environments. See Mersch (2018).

Payment options are being embedded into value processes, called "invisible payments," and smart assistant solutions, such as voice first or virtual reality (with improved natural language processing and image recognition), which offer applications for payments initiation and acquisition. Contactless and open payments are rapidly gaining importance, forcing providers to upgrade their service and business models. Open payment platforms are open-source networks that offer transparent and freely available APIs. They can be used, distributed, improved, and further developed by third parties without any restrictions. Under open payment regulations, banks are required to provide access to current accounts to third parties, PSPs, and information service providers.

Competition is growing from digital "disruptors," which provide initiation and account information services. The emergence of distributed ledger technology and the global payments innovation (GPI) initiative by SWIFT are revolutionizing cross-border payments, enabling transactions to be executed within minutes.

Distributed ledger technology is a tool for recording ownership. A distributed ledger is a database of transactions that is spread across a network of many computers, rather than stored in a central location. It is consensually shared and synchronized across multiple sites, institutions, or geographies. A participant at each node of the network can access

the recordings shared across that network and own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.

SWIFT GPI is a new facility that enables quicker payments with full transparency on accompanying costs while providing on-the-spot information about the status of transactions. With GPI, a payment is effective on the same day the payment process is initiated, and a breakdown of all of the costs involved in the payment, including exchange-rate costs, is provided to the party initiating the payment. The status of the payment situation with respect to correspondent banks is available at all times. This traceability is possible due to a unique reference associated with each payment that is kept and shared by the different banks involved in the operation. The process finalizes with confirmation that the payment has been deposited in the beneficiary's account. Information regarding the payment remains unchanged and homogeneous during the process, and details provided by the issuer are the same as those received by the recipient as a result of the commitment established between the banks taking part in SWIFT GPI. These technologies facilitate end-to-end tracking of payments (just like tracking a courier), offer transparency, and allow companies to optimize liquidity.

New technologies provide alternatives to (costly) card payments, which still dominate the retail payments landscape globally (and especially in advanced economies) for routine day-to-day purchases; in that respect, they offer important opportunities for leapfrogging in emerging markets. New technologies also permit the adoption of simplified payment processes, and others help to address the shortcomings arising from the lack of sufficient control, flexibility, and transparency in current payment mechanisms.

As an example, the New Payments Architecture initiative in the United Kingdom will bring in, among other things, a new overlay service called the "Request to Pay," that will enable the shift from traditional pull payment models, such as direct debits, to push payment models, thereby simplifying the payments workflow and increasing customer control. This will phase out mandate management and provide indemnity from reversals. Note, however, that mandate management might still be necessary for pre-agreed recurring payments (such as mortgage repayments).

Finally, the growing flow of information associated with DPS has expanded the possibilities for data analytics and higher automation and facilitated the development of new data-rich and personalized products and services.

ANNEX 2

THE EVOLUTION OF PAYMENTS AND PAYMENT REGULATIONS

Regulations in the payments business have evolved as payment technologies have changed. While the execution of payments had long been ancillary to the management of bank accounts, and the monitoring of payments activity had been deemed a part of banking supervision, the first significant change was the recognition that governing payment systems and services was a distinct central banking activity. Systemic risk and efficiency considerations led central banks and the banking industry to establish new centralized payment infrastructure. New systems and institutions (for example, payment-system operators, network service providers) became primary actors. Clearing houses were established, where transactions could be executed under a multilateral scheme, and real-time settlement systems were conceived for high-value transaction, permitting immediate transfers and replacing correspondent banking as the typical infrastructure for interbank transactions, while for lower-value transactions new systems were developed to allow for the execution of credit-based transfers with deferred settlement at the end of the business day. Concepts such as netting, finality, and collateral became the objects of specific regulatory and policy attention, focused on safeguarding systems and protecting them against spillovers. In particular, as banks would commonly be exposed to domino effects if one of the banks defaulted on its obligations to the others, central banks focused on "payment systems" as specific entities to regulate and elaborated standards and rules to mitigate systemic risk. Payment-system "oversight" emerged as a central banking activity that would be complementary and yet separate from banking and financial supervision.

At the retail level, with the first wave of retail payment service innovation—that is, the digitization of bank accounts (see appendix A)—new payment instruments (such as debit and credit cards, electronic transfers) and channels (such as the Internet and mobile banking) developed. However, they were all linked to bank accounts, and regulation and policy remained directed at banks and did not require fundamental changes, except recognizing that payment instructions could be made electronically. Execution of payment services was factually the realm of banks. Under the given stage of technology and business model, the focus of regulation moved from solely payment systems to payment services and the issuance and management of payment (card) instruments. Within such context, no autonomous oversight of payment service existed, and the issuance of payment instruments was under the purview of banking supervision.

As technology deepened, the capability was developed for storing monetary value in electronic devices (such as chips and computers), followed by the concept of a prepaid account that is distinct from a bank account. Payment services could therefore be provided by non-bank entities without the need for customers to hold accounts with banks. This led to new instruments such as e-money and then mobile money, and it eventually opened the door for non-banks to become issuers or acquirers and for new individuals and businesses to act as third-party agents for banks and non-banks wanting to intercept clients in places where establishing brick-and-mortar structures would be too expensive. The second wave of innovation was thus the recognition of payment services as a distinct activity that could be provided as a service separate from bank accounts. (See appendix A.) As a consequence, the focus of regulation had to extend to non-bank PSPs and instruments, and the scope of oversight expanded to cover retail payments. Payments became an activity that (at least in principle) could be regulated autonomously and open to all entities that obtain a prior authorization or license from the relevant authority. In some jurisdictions, new categories of financial entities (for example, the "Payment Institutions" in the European Union) were permitted to provide payment services upon authorization (mainly, under a licensing mechanism). Also, new authorities started to play an enlarged role, such as the agencies responsible for telecommunication, consumer protection, competition and market conduct, market integrity, and security.

Several jurisdictions initially moved gradually and adopted so-called bank-led regulatory models, whereby non-bank providers could operate (and new services could be made available to customers) only through banks, while other jurisdictions permitted non-banks to enter the market in partnership with banks or took a liberal approach, letting non-banks compete with banks. Technology, however, has progressively extended and diversified the value chain in the supply of payment services, making it possible for a multitude of entities to specialize in, and compete for, the provision of services within and across each segment of the long chain.

As most jurisdictions eventually embraced the non-bank-led models, the notion evolved that *the initiation of payments could be delinked from the maintenance of accounts*—the third wave of innovation (see appendix A)—and could be provided by any entity and linked to any account (based on customer consent). This is the world of open banking, APIs, and tokenization, leading to greater competition in DPS provision and paving the way for all (appropriately licensed) entities to establish relationships with customers for the provision of DPS without necessarily operating their accounts. As it clearly appears, the activities that underlie payments execution in the digital era are quite different from the traditional services the industry initially produced. And while much of the action originally revolved mainly around interbank clearing and settlement, today such activities represent just one small (although extremely relevant) component of a much more composite picture. Moreover, and very importantly, the new picture has implied an overall reshaping of the market for the provision of payment services and a major reconsideration of the associated risks, giving prominence to the need to regulate competition and to engage the appropriate authorities in this regard. (See section IV.B in the main text.)

The latest wave of innovation—that is, *the delinking of accounts altogether from payments (see appendix A)*—brings us to the world of crypto-assets, cryptocurrencies,

and their subset of stablecoins. In principle, crypto-assets can be divided into those that do not represent any real-world asset (for example, cryptocurrencies) and those that are a representation of real-world assets or have the backing of an institution (for example, stablecoins). In practice, the world of crypto-assets is fluid; hundreds of innovations are made every month, and new products combine different features of crypto-technology and distributed ledgers. Authorities worldwide are evaluating the implications of these innovations and how new regulations and oversight instrument should be adapted to protect systems and consumers from risks without stifling competition and further innovation. Particularly active in this area are international organizations and standard-setting bodies such as the Financial Stability Board, various committees of the Bank for International Settlements (including, importantly, the Basel Committee on Banking Supervision and the Committee on Payments and Market Infrastructures), the International Monetary Fund and World Bank, the International Organization of Securities Commissions, the Financial Action Task Force, and the Organisation for Economic Co-operation and Development.

ANNEX 3

MENA FINANCIAL INCLUSION FOR YOUTH AND WOMEN

TABLE C1: MENA FINANCIAL INCLUSION FOR YOUTH (15–24 YEARS OLD) AND ADULTS (25 YEARS OLD AND OLDER) BY REGION

		World	East Asia & the Pacific	Europe & Central Asia	Latin America & Caribbean	Middle East & North Africa	South Asia	Sub-Saharan Africa
No deposit and no withdrawal from an account in the past year	Youth (%)	18	22	15	19	24	43	30
	Adults (%)	13	19	12	21	18	42	26
Mobile money account ownership	Youth (%)	15	8	9	7	5	6	25
	Adults (%)	13	6	5	7	4	5	24
Made or received digital payments in the past year	Youth (%)	33	37	30	21	15	10	33
	Adults (%)	36	29	25	16	13	10	33
Account at a financial institution	Youth (%)	40	45	38	34	25	42	24
	Adults (%)	63	58	66	51	46	56	33
Saved at a financial institution	Youth (%)	15	18	9	11	7	10	10
	Adults (%)	26	24	14	14	12	17	13
Borrowed from a financial institution	Youth (%)	6	8	8	7	3	4	5
	Adults (%)	14	18	14	13	9	9	8

TABLE C2: MENA FINANCIAL INCLUSION FOR YOUTH (15–24 YEARS OLD) BY GENDER AND REGION

		World	East Asia & the Pacific	Europe & Central Asia	Latin America & Caribbean	Middle East & North Africa	South Asia	Sub-Saharan Africa
No deposit and no withdrawal from an account in the past year	Female (%)	19	21	17	20	26	48	33
	Male (%)	17	21	13	18	23	39	28
Mobile money account ownership	Female (%)	13	8	7	5	4	2	22
	Male (%)	17	9	15	8	5	10	28
Made or received digital payments in the past year	Female (%)	31	38	27	18	14	5	30
	Male (%)	35	34	36	24	16	14	36
Account at a financial institution	Female (%)	37	47	38	33	21	35	21
	Male (%)	42	42	45	37	32	48	26
Saved at a financial institution	Female (%)	13	17	8	9	6	9	8
	Male (%)	16	18	10	12	9	12	11
Borrowed from a financial institution	Female (%)	6	9	8	7	2	3	4
	Male (%)	7	7	9	7	3	4	5

Source: Anderson, Hopkins, and Valenzuela (2019).

ANNEX 4

BARRIERS TO ENTRY IN DPS MARKETS[123]

Barriers to entry in DPS markets may arise from regulatory requirements (licensing of the activity), the strategic behavior of incumbents (access to essential inputs), or consumer behavior. This appendix focuses on the last two types of barrier.

Strategic Barriers

In many jurisdictions, there is a risk that incumbent operators, typically banks, may foreclose on new providers. In fact, new entrants may provide their services only if banks grant them access to the existing inputs, such as account information or banking infrastructures (clearing and settlement system), whose access is subject to regulatory requirements. In fact, banks tend to see client account data as their exclusive property.

Front-end and end-to-end PSPs may face greater entry and expansion barriers, as they need to access client account information and, in the case of end-to-end operators, to the clearing and settlement system.

The risk of foreclosure stems from the fact that the inputs needed by new PSPs are possessed by operators (banks) that compete with them in some services. For example, to provide payment-initiation services, new fintech operators today can execute services that previously were provided by banks. As such, the arrival of new PSPs may jeopardize the relation between the clients and their banks, as the new PSPs gain front-end interaction with the clients. Therefore, and taking into account the cross-selling strategy undertaken by banks, the loss of front-end contact with the client may have consequences for other bank products or services. The risk of foreclosure to front-end PSPs lies essentially with the access to account data, for these kinds of providers do not settle payments.

In the case of end-to-end services, other than the access to account information, new PSPs may also experience difficulties accessing payment infrastructures, such as clearing and settlement systems. Access to these infrastructures is typically indirect, whereby the PSPs access the systems through a payment account held with banks. Yet indirect access could pose a foreclosure risk, since the PSPs must establish relationships with the banks that happen also to be their market competitors.

Direct access by non-bank PSPs to the clearing and settlement system would make them less dependent on banks, which would benefit competition. Yet regulatory barriers that prevent direct access exist in many jurisdictions today.

Another type of barrier would exist when banks own such basic infrastructures as ATM networks and exclude non-bank PSPs from accessing and using them.

Barriers Arising from Consumer Behavior

Some aspects of consumer behavior are likely to act as a barrier to entry by limiting the ability of new market players to expand their activity. It should also be noted that some of these demand behavior aspects may be induced or promoted by incumbents' strategies (for instance, bundling and cross-selling). Moreover, in two-sided markets, consumer resistance to new services also affects the attractiveness of such services to retailers.

Low consumer mobility in retail banking and low financial literacy are typical entry barriers in the financial sector. In the case of fintech services, in addition to financial-literacy aspects, consumers may not be receptive to new products and services due to digital-literacy issues.

The propensity of consumers to adopt new patterns of payment-service consumption—namely, by using technology-based services—may be influenced by other factors related to behavioral aspects or information asymmetries. These factors include product/service knowledge, adjustment costs, trust in products/services, perceptions of security, and reluctance to share data. Some stakeholders mentioned that a lack of consumer trust in, for example, mobile payments is also an entry and expansion barrier.

ANNEX 5

RISKS OF MARKET FORECLOSURES TO FINTECH OPERATORS IDENTIFIED BY THE EUROPEAN COMMISSION AND OTHER COMPETITION AGENCIES[124]

On October 3, 2017, the European Commission conducted inspections in some member states due to concerns that banks and banking associations were breaking European competition law by preventing third-party providers from having access to account data to which account holders had given their consent (EC 2017).

In March 2018, the Brazilian Conselho de Administração de Defesa Económica opened an inquiry into an alleged refusal or limitation of a fintech firm's access to account information by five banks through excessive prices.[125]

In December 2017, the Dutch Autoriteit Consument en Markt (ACM) published a study on the risk of market foreclosure by banks to fintech firms (ACM 2017). With regard to front-end fintech operators, the ACM concluded that banks have market power and the incentive to foreclose access to client account data. As regards end-to-end fintech operators, the ACM did not identify any risks of foreclosure by banks of the indirect access of fintech operators to the clearing and settlement system, given that (i) it is highly unlikely that banks have upstream market power over payment accounts and (ii) the revised Payment Services Directive (PSD2) establishes that indirect access must be granted in a non-discriminatory, objective, and proportional manner. With respect to the direct access of end-to-end fintech operators to the clearing and settlement system, the ACM believes regulatory changes are in order to establish a banking license right that allows them direct access to the infrastructure under certain conditions.

In December 2017, the Canadian Competition Bureau published a study that identifies issues arising from fintech PSPs' access to banking services, because fintech operators are at the same time clients and competitors of banks (Competition Bureau Canada 2017). Following public consultation, stakeholders mentioned the difficulty they experience gaining access to the basic banking services they need to operate—namely, service delays and disruptions/termination. The bureau concluded that incumbents may indeed foreclose access to new fintech players.

In a study of retail banking published in 2016, the United Kingdom's Competition and Markets Authority put forward a package of remedies to promote competition in the sector, including the open banking initiative, consisting of measures aiming to ensure transparency in banking services, the assessment of service quality, and open bank APIs, so as to ensure that fintech players have access to the necessary inputs (CMA 2016).

In 2016, the German competition authority (Bundeskartellamt) deemed some online banking rules to be anticompetitive because they limit the access of non-bank financial institutions to the payment system.[126]

The Icelandic competition authority (Samkeppni) reached an agreement with two of the country's leading banks on measures to enhance competition in the retail banking market. Among these measures, the two banks must provide information with regard to any charges, fees, and terms through an open API, so that fintech operators may compare the service conditions offered to clients.[127]

In October 2017, the Mexican Comisión Federal de Competencia Económica provided an opinion on draft legislation to regulate fintech service providers[128] and recommended (i) a reduction in the authorization/licensing time limits; (ii) the introduction of regulatory sandboxes; (iii) an open and non-discriminatory access to account information by third-party providers; (iv) technological neutrality; and (v) regulation that is proportional to the risks of the activity.

ANNEX 6

G20 POLICY GUIDE: KEY RECOMMENDATIONS

DIGITAL ONBOARDING

Improve the identification and verification of new customers

1) **Ensure an integrated identity framework**
   A digital legal identity system could help recognition and authentication.

2) **Adapt and upgrade the regulatory framework**
   A conducive regulatory framework should recognize the potential of digital identity.

3) **Establish a robust and secure digital identity infrastructure in the financial sector**
   Digital identity systems could be built and used in the financial services industry.

4) **Foster development of private sector–led services by leveraging legal identity infrastructure**
   The private sector could build innovative solutions.

5) **Monitor new developments and approaches to identity**
   Regulators should stay abreast of technological developments.

DIGITAL PAYMENTS INFRASTRUCTURE

Build an open and inclusive payments ecosystem

1) **Prioritize development of interoperable payment systems enabling fast payments**
   Policy makers should establish a market-based, safe, efficient, and interoperable payment system.

2) **Create incentives for merchant payments acceptance**
   Business models should be sustainable while promoting use by merchants.

3) **Create incentives for consumer use of DFS**
   Use by final consumers should be affordable.

4) **Support cross-border payment systems**
   The development of cross-border approaches could be explored.

USE OF ALTERNATIVE DATA FOR CREDIT REPORTING

Leverage alternative data to enhance credit reporting

1) **Improve the availability and accuracy of information**
   The main categories of alternative and reliable data should be identified.

2) **Expand credit information sharing**
   Credit information sharing could be extended to alternative data.

3) **Enable responsible cross-border data exchanges**
   Regional cooperation could help improve the consistency and comparability of data.

4) **Balance market integrity, innovation, and competition**
   Functional requirements should be applied to ensure quality of treatment

FINANCIAL CONSUMER PROTECTION, FINANCIAL LITERACY, AND DATA PROTECTION

Increase opportunities while mitigating risks

FINANCIAL CONSUMER PROTECTION

1) **Adapt oversight arrangements and capability for financial consumer protection**
   Regulators should embrace technology while keeping high standards of consumer protection.

2) **Enhance disclosure and transparency**
   Technology could be leveraged to adapt and strengthen disclosure and transparency standards.

FINANCIAL LITERACY

3) **Foster data collection and coordination and the identification of new core competencies on digital financial literacy.**
   New data should be used to identify competency frameworks in a coordinated manner.

4) **Strengthen the delivery of financial education for DFS and support its evaluation**
   Digital technology could be leveraged for the provision and evaluation of financial-education programs.

DATA PROTECTION

5) **Enhance secure and effective consent models**
   Consent models could be adopted to ensure data protection.

6) **Enhance access, rectification, cancellation, and opposition rights**
   Consumers should be given options to access and change their own data.

7) **Address data security**
   Adoption of security measures could help protect against operational risks.

Source: GPFI (2018).

ANNEX 7

OTHER DPS-BASED POLICY RESPONSES TO CRISIS SITUATIONS

This appendix presents a list of policy measures aimed at encouraging and supporting the use of DPS during crises. Efficient and effective delivery of DPS, however, requires that payment and settlement systems continue to operate safely and efficiently during crises. The appendix, therefore, also includes a list of policy measures designed for this purpose.

Measures to Support DPS

Quickly deploy DPS solutions tailored for vulnerable and financially excluded populations.

- Identify non-cash payment services that are critical during a crisis and work to ensure that they remain fully functional. To do so, the following criteria could be used:
  - Usage by the most vulnerable segments of the population
  - High level of adoption among the population
  - Low level of human interaction required to use the payment service
- Ensure that transaction-processing systems (that is, the switches, transaction-authorization mechanisms, and payment clearing and settlement systems) have sufficient capacity to support a surge in the usage of some DPS.
- When mobile-money services are considered critical, support users by taking the following steps:
  - Engaging with network telecommunication and connectivity providers to implement a temporary elimination of data charges for mobile payment services
  - Engaging with telecom regulatory agency to enable the use of USSD for bank-issued mobile wallets
  - Partnering with telecom providers to ensure that transfer instructions could be transmitted with minimal connectivity requirements
- When card payments are labeled as critical payment services, support users by taking the following steps:
  - Withdrawing requirements to authenticate identity by means of personal identification numbers (PINs) for low-value payments in order to avoid contact with POS terminals or other card-accepting devices

  - If possible, enabling the contactless functionality of cards and card-accepting devices

- Consider temporarily modifying authentication mechanisms for low-value payment instruments/devices in order to facilitate their usage at merchant locations. For example, for low-value payments with cards at merchants, consider eliminating the need to key in a PIN.

- Recommend or mandate a temporary reduction of fees on critical payment services as a way of supporting the users and the smooth functioning of the economy, as has been done by the Central Bank of Egypt. Immediate implementation of these provisions is essential. However, when establishing the duration and size of the decrease, authorities should consider the following:
  - The risk of those costs being shifted elsewhere in the ecosystem
  - The cost to compensate the operator of the payment service

- Without creating AML/CFT concerns, temporarily increase transaction and balance limits for certain transaction accounts or payment products, especially those that are used by population segments that are more vulnerable to the crisis impacts, as has been done by the Central Bank of Egypt. Immediate implementation of these provisions is essential. In this regard, the authorities should also consider the following:
  - The potential effects on liquidity/cash availability at access points if a vast number of end beneficiaries decide to cash out
  - Require all businesses offering essential services—pharmacies, hospitals, and grocery shops—to accept digital payments irrespective of the purchase amount and without any customer surcharge.

- For mobile-money payment services, support users by engaging with MNOs to implement a temporary elimination of data charges specific to mobile-money transactions.

- Promote immediate enrollment of new merchants that will be accepting digital payments.

- Simplify onboarding requirements for agents, without creating AML/CFT concerns, to enable onboarding of essential businesses as new agents.
  - As the country closes all non-essential businesses, many agents that are in this category need to close as well. This reduces the availability of the cash-in/cash-out points in the short term.
  - This is an essential measure in order to keep a widespread cash-distribution network.

- Simplify merchant onboarding requirements. For example, engage with acquirers to offer remote and immediate enrollment of merchants through simplified KYC. A simplified or contingency account could be used to receive payments. (See below for a proposal for a contingency account.)
  - The distribution of free, temporary, mobile POS terminals or other transaction-accepting devices should be considered. Consider solutions with contactless features if contactless operation is enabled in the ecosystem.

  - Work with DPS providers and switches to develop easy-to-use services that can be conducted in line with social-distancing norms—for example, a one-time-password solution to use at merchants that could serve as a solution to in-person and e-commerce transactions.

- Consider implementing additional measures to provide cash transfers to vulnerable population segments via digital payment instruments.
  - Measures could be taken to provide cash transfers to the segments of the population that are most severely affected by crisis-related restrictions (for example, workers in the informal sector, workers who are unemployed due to the crisis, receivers of remittances who are no longer able to receive payments from abroad).
  - Choosing and onboarding beneficiaries would benefit from the availability of a national registry and the use of national ID cards with unique ID numbers.
  - For social cash transfers, where feasible, transfers to current and new beneficiaries should be migrated to transaction accounts in order to reduce the need for people to leave their homes to get their money and, even more importantly, to use cash altogether.
    > Ensure the availability of cash-out services, and closely monitor points of access in areas where vulnerable groups are located.
    > Avoid overcrowding at these distribution networks: identify normally overcrowded cash-out points and spread cash-outs. Effective communication with beneficiaries is essential for this purpose.

Create awareness and ensure protection of DPS users.

- Conduct widespread awareness campaigns and basic financial/digital-literacy programs. These should include basic information to be broadcast on national TV/radio. Social media are another effective channel.
- Inform the public about all the policy actions taken for non-cash payment services and other related matters.
- Consider warning the public against phishing messages related to the crisis.
- Ensure financial consumer protection. It is important that related provisions be extend to all DPS providers (not just banks), as well as all the services and features added for crisis-related purposes, such as automatic enrollment to Internet banking.

Basic Measures to Support Payment and Settlement Systems

Avoiding operational disruptions of critical payment systems

- Ensure that business continuity plans guarantee the operational continuity of all the critical elements of a system (that is, hardware, software, network, participant interfaces, transaction monitoring, physical and logical security, and so on). Also, coordinate with other authorities and critical service providers to secure the provision of network, electricity, and other relevant services.

- Ensure that operating a payment system in contingency mode does not exacerbate cyber risks. (For example, if needed, introduce additional/more robust controls for remote access and IT security briefings.)
- Prepare to support payment systems operated by the private sector by sharing technological and human resources (for example, putting in place collaborative spaces and facilities).
- Ensure the efficacy of crisis decision-making and internal and external communication protocols of critical payment systems, including for potential scenarios under COVID-19 (for example, countering fake news that is being spread through social media).

Avoiding or mitigating credit or liquidity events in payment systems

- Reassess risk-management tools for credit and liquidity risks of payment systems (for example, collateral arrangements, limits, participant default arrangements, and so forth) to ensure they are robust.
- In line with the overall monetary policy and fiscal policy measures, assess or reassess the specific needs of critical payment-system participants regarding access to sources of liquidity.
- Just as with operational risks, ensure the availability and efficacy of crisis decision-making and internal and external communication protocols.

ENDNOTES

1 The fourth wave (that is, the delinking of accounts from payments leading to crypto-assets and cryptocurrencies) comes with many potential issues that are still being studied, and, in any case, the adoption of the associated digital payment services (DPS) is predicated on such issues as know your customer (KYC), merchant acceptance, agent networks, and consumer protection, which are common to the first three waves. Furthermore, it is not still clear at this stage whether this fourth wave of innovation should be part of an overall strategy for DPS.

2 In usage, this report will distinguish between the terms *digitization* and *digitalization*. The former will be used to refer to cases where technology is introduced in a process or business for the purpose of rendering analog records, processes, and actions in digital form. The latter will be used, more broadly, to refer to a process or business that is reengineered in a way that is cognizant of contemporary technologies built to suit modern customers and delivered, at least in part, through digital means and channels. Thus, while *digitizing* is about business efficiency and effectiveness, *digitalizing* concerns business transformation and implies the transition to a digital environment. The latter is, in fact, the subject of this report, as it applies specifically to developing sound and dynamic DPS ecosystems in the Middle East and North Africa (MENA) region.

3 Fintechs operating in the payments space{-OK?-} cover a wide range of services. Examples of such services include mobile payments for merchants; solutions using chip and personal identification number debit and credit card payments via smartphone or tablet devices; solution enabling online businesses and services to accept card payments on their websites; solutions for online retailers that allows them to offer payments options to customers; solutions to secure and process online bill and recurring payments; platforms enabling customers to purchase online; platforms that automate debt management for individuals and companies; online processors that power one-click payments for consumer apps; solutions that help corporate businesses to organize and optimize their payment and cash-management processes; open- and closed-loop cards and online-based payments from cobranded prepaid cards for consumers; solutions to accept payments in online shops; tools and technologies for customer loyalty across every marketing channel (in store, online, mobile); developments of application programming interfaces (APIs); platform-as-a-service payment infrastructures that enable providers to outsource their entire payment processes; mobile payment platforms enabling merchants to offer mobile point-of-sale (POS) solutions to customers; secure payment platform for e-commerce companies; and solutions to secure digital payment methods for business-to-business commerce.

4 The "gig economy" refers to an economy where the labor market is characterized by the prevalence of short-term contracts or freelance work, as opposed to permanent jobs. The expression "app economy" indicates the range of economic activity surrounding mobile applications. The app economy encompasses the sale of apps, ad revenue, or public relations generated by free apps and the hardware devices on which apps are designed to run. The well-known word *blockchain* literally means a chain of digital blocks (which store information) and technically refers to an immutable time-stamped series record of data that is distributed and managed by a cluster of computers. Finally, the "Internet of Things" is a computing concept describing everyday physical objects that are connected to the Internet and able to identify themselves to other devices.

5 For many people, today's increase in access to digital finance brings more choice and greater convenience and enables the "pay as you go" model for essential services, such as electricity and water. Through inclusion, efficiency, and innovation, access opens to poor and disadvantaged clients prospects that were previously out of reach. As an example, in a number of countries, digital lending platforms and new entrants have entered market segments where they have no competition from the incumbents, providing online services to unbanked or underserved clients such as small businesses, subprime customers, and clients with insufficient credit history or lower job security who cannot apply for loans from traditional players.

6 Finality in payments (or final settlement of payments) is defined as the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the transferor to the transferee in accordance with the terms of the underlying contract. Final settlement is a legally defined moment.

7 The idea that a well-working financial system plays an essential role in promoting economic development dates back to Bagehot (1873) and Schumpeter (1911). Empirical evidence for the relationship between finance and growth is more recent. Goldsmith (1969) was the first to show the presence of a positive correlation between the size of the financial system and long-run economic growth. In the early 1990s, economists started working toward identifying a causal link going from finance to growth. King and Levine (1993) were the first to show that financial development is a predictor of economic growth. More evidence in this direction came from Beck et al. (2000), who used different types of instruments and econometric techniques to identify the presence of a causal relationship going from finance to growth. Finally, Rajan and Zingales (1998) provided additional evidence for a causal link going from financial to economic development by showing that industrial sectors that, for technological reasons, are more dependent on finance grow relatively more in countries with a larger financial sector. By now, an enormous literature shows that finance does indeed play a positive role in promoting economic development, and few economists now doubt the existence of such a causal link (Levine 2005). The global financial crisis raised concerns that some countries may have financial systems that are "too large" compared to the size of the domestic economy (Arcand, Berkes, and Panizza 2015; Zhu, Asimakopoulos, and Kim 2020).

8 A mobile wallet is a virtual wallet that stores payment card information on a mobile device. Mobile wallets can be used to make in-store payments and payments at merchants listed with the mobile wallet service provider. The mobile wallet is an app that can be installed on a smartphone, or it is a feature built into a smartphone. The mobile wallet stores credit card, debit card, coupons, or reward card information. Once the app is installed and the user inputs payment information, the wallet stores this information by linking a personal ID format, such as a number or key, a QR code (see below), or an image of the owner,

to each card that is stored. When the user makes a payment to a merchant, the mobile app uses a technology called near-field communication (NFC), which uses radio frequencies to communicate between devices. NFC uses the personal ID format created for the user to communicate the payment information to the merchant's POS terminal. The information transfer is usually triggered when the user waves or holds an NFC-enabled mobile device over the store's NFC reader. Not all smartphones or mobile devices are equipped with NFC technology, including the iPhone device. For iPhone users, there are alternative ways to use their mobile wallets to make in-store payments. PayPal's mobile wallet allows users to make payments using their mobile phone numbers during checkout. The phone number has to be linked to the user's PayPal account for the transaction to be approved. The QR code is a two-dimensional version of the barcode, known from product packaging in the supermarket. The QR code has found its way into mobile marketing with the widespread adoption of smartphones. QR stands for "quick response," which refers to the instant access to the information hidden in the code. QR codes are gaining popularity because the technology is "open source"—that is, available for everyone. Significant advantages of QR codes over conventional barcodes are larger data capacity and high fault tolerance.

9 The expression "digital channels" refers to the Internet, mobile phones (both smartphones and digital feature phones), ATMs, POS terminals, NFC-enabled devices and near sound data transfer devices, chips, electronically enabled cards, QR codes, biometric devices, tablets, phablets, and other digital systems. DPS can expand the scale, scope, and reach of financial services and promote efficient interconnection among participants in economic activities; they contribute to reducing costs and information asymmetries, increasing efficiency and competition in financial and goods markets, and widening access to financial services. They thus support economic development and are essential to closing the gaps in financial inclusion.

10 For an extensive discussion of fostering the usage of financial services by women as a public policy, see Toronto Centre (2018).

11 An API is a set of protocols and tools that underlie application software programming. An API defines how software components communicate with one another. An open API enables external app developers to establish communication between their own apps and the apps and information systems of the entity providing the open API. In the case of payment services, a credit institution that uses an open API will be providing a digital platform that allows third-party providers access to the account data and services it provides to its clients, provided the client has given his consent. For example, when a client places a payment order through a mobile app developed by a fintech service provider, the client's bank will be obliged to grant the fintech provider access to its client account data for the payment to be made. Also, APIs that allow non-financial organizations to connect to payment service providers (PSPs) can facilitate automated payments in the Internet of Things context (for example, cars automatically paying an insurance premium in a pay-as-you-go model; objects automatically paying for the energy they consume; refrigerators sending shopping lists along with payment credentials to an online grocery delivery store; or in pay-per-use object-sharing models). Finally, financial market infrastructures and critical service providers generally publish API specifications to enable direct connections between their clients' back-office systems and their own information systems. These direct connections could lead to greater transaction-processing efficiency, including enabling straight-through processing.

12 Tokenization is the process of protecting sensitive data by replacing it with an algorithmically generated number called a "token." In credit card tokenization, the customer's primary account number is replaced with a token. As a payment is processed, the token is passed through the Internet or the various wireless networks processing the payment, without actual bank details being exposed. The actual bank account number is held safe in a secure token vault. Tokenization is typically used to prevent credit card fraud.

13 Distributed ledger technology (DLT) refers to the processes and related technologies that enable nodes in a network to securely propose, validate, and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes (CPMI 2017). A "crypto-asset" is a type of private asset that depends primarily on cryptography and distributed-ledger or similar technology as part of its perceived or inherent value (FSB 2019a). A "cryptocurrency" is a digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrencies use DLT as opposed to centralized systems for the execution, clearing, and settlement of payments. A "stablecoin" refers to a class of cryptocurrencies that are designed to minimize the volatility of their price relative to some stable asset or basket of assets. A stablecoin can be pegged to a cryptocurrency, fiat money, or exchange-traded commodities (such as precious or industrial metals). Stablecoins redeemable in currency, commodities, or fiat money are said to be "backed." Stablecoins have gained traction, as they attempt to offer the instant processing as well as the security and privacy of cryptocurrencies and the stable value of well-managed fiat currencies.

14 As defined by the Organisation for Economic Co-operation and Development (2017), "big data" is commonly understood as "the use of large-scale computing power and technologically advanced software in order to collect, process and analyze data characterized by a large volume, velocity, variety and value." Consumer data stemming from online behavior, geolocation tools, digital payments, and wearables is fueling a gold rush in several industries worldwide and affecting consumers' daily financial lives in terms of product choice as well as privacy and data protection.

15 See World Bank (2017) for a more complete discussion of the applications.

16 In some countries, users transact by giving cash to PSP agents for the latter to make digital payments on their behalf.

17 Such attributes include, among other things, simplified account-opening procedures for low-risk, low-value transactions, a low fee structure (on a per-transaction basis), the absence of a minimum balance requirement, the use of transaction accounts remotely and at agent locations (instead of bank branches), access to digital financial and commercial services, and easier access to credit, owing to the data trail that these accounts make possible. Another key attribute of DPS that can facilitate financial inclusion is that a new class of players may be more motivated than traditional banks to make them available to the financially excluded. For a comprehensive treatment of payment services in the context of financial inclusion, see CPMI-World Bank Group (2016), also known as the PAFI (Payment Aspects of Financial Inclusion) Report. For additional guidance on recent fintech developments that have relevant implications for PAFI's underlying objectives, see CPMI-World Bank Group (2020).

18 More specifically, the three types of process breakpoints can be described as follows:

- *Technology failure:* This type of process breakpoint includes issues such as transaction delays due to a poor cell-phone signal, back-end issues with the core technology, an agent's phone or terminal not working, the failure of a system to send a text confirming a transaction, or a lack of signal due to towers being down following an earthquake. Note that this does not include technology failures due to malfeasance. With increasing digitization of processes, the number of technology-linked breakpoints is expected to grow.
- *Human error:* This includes issues such as an agent or customer inputting the wrong account number or menu selection, or an agent or customer accidentally providing the wrong amount of cash. It also includes instances when agents do not carry out their intended role due to external factors (for example, sickness, protest, or bankruptcy of their employer). Human error can also occur at the main provider offering the service (for example, when a call-center agent accidentally misinforms a customer or transfers the wrong amount of money in a manual process or override).
- *Malfeasance:* This includes fraudulent and/or illicit activities, such as agents stealing from customers; customers stealing from agents; third-party actors stealing from customers, agents, or providers; or individuals intentionally tampering with core infrastructure, such as cutting critical fiber-optic cables.

19 Each breakpoint falls along a continuum, from those affecting a single customer to those affecting all customers. For example, in the person-to-person (P2P) remittance process, a dropped connection that

delays a transaction is a technology risk affecting a single customer. By contrast, failure of a digital money operator's entire back-end system affects all customers' ability to transact. Other breakpoints affect an intermediate number of customers. For example, in the case of a power outage at a cell-phone base station, customers within that tower's coverage radius are unable to transact until the tower is functioning again.

20 See Smith et al. (2011).

21 The contents of this paragraph draws on HelpAge International (2012).

22 Of course, corruption and leakage can still occur with e-payment systems. If recipients have been registered erroneously or fraudulently, a unique identifier will not eliminate this kind of leakage. Ensuring that payment agents do not make additional charges has been a challenge for Pakistan's flood response and other cash-transfer programs.

23 For example, a criminal might call a bank customer, tell her that her account has been compromised, and help her to transfer money to a supposedly safe account that is actually under the criminal's control.

24 This prompted the United Kingdom's Payment Systems Regulator in 2018 to undertake a public consultation on an industry code for the reimbursement of victims of so-called authorized push-payment scams, where victims are tricked into sending money to a fraudster. The code, which has been designed to help prevent such scams and give people better levels of protection, has been developed by representatives from the banking industry, other PSPs, and consumer groups.

25 A striking example is the mobile payments market in China, where two firms account for 94 percent of the overall market. The implications of fintech development for the market structure of financial services are extensively analyzed in FSB (2019b).

26 This paragraph draws on BCBS (2018).

27 Innovative technologies can help financial institutions comply with regulatory requirements and pursue regulatory objectives—prudential requirements including reporting, consumer protection, and anti-money laundering and countering the financing of terrorism (AML/CFT). In this context, regtech may provide PSPs with more effective ways to improve their compliance and risk management, and it may also be a means of coping with change in the regulatory environment and driving down the costs involved in meeting the corresponding requirements. Regtech could result in new processes, new distribution channels, new products, or new business organizations that help PSPs comply with regulatory requirements and manage risk more effectively and efficiently. Some regtech firms offer compliance and risk-management solutions to PSPs, through outsourcing or insourcing processes. Examples include the FundApps automated monitoring service for regulatory changes in the United Kingdom and Fintellix in India, which offers data management for compliance with accounting rules. Regtech may open up opportunities for digital transformation of control-and-support functions within banks (risk, compliance, legal, finance, IT). Regtech could address a wide array of requirements related to regulatory reporting, financial crime, operational risk (including cybersecurity and fraud detection), consumer protection and data-protection regulation. Examples in these domains include BearingPoint's Abacus solution for compliance with the European supervisory reporting requirements and Trulioo's and Qumran's KYC solutions in Canada and Switzerland, respectively, for compliance with AML/CFT rules. In Italy, AML requirements for the opening of a new online account can be met by making a transfer from any bank account the customer holds at any other bank. All other necessary information and documents can be exchanged between the customer and the PSP using e-mail, webcam, chat, and other online tools. The technologies used include IT (software, cloud computing, API, automation, and artificial intelligence), data technologies (big data, machine learning, risk scoring, real-time monitoring), identity technologies (biometrics, vocal recognition), or new technologies such as the DLT that combines cryptography and IT solutions. Another potential use of regtech includes risk-data-reporting capabilities. During the financial crisis, firms were unable to aggregate risk data and perform analytics to aggregate risk exposures in response to events in a timely fashion. Regulators have placed increased expectations on firms to be able to aggregate risk data accurately and completely, with a view to improving their risk management and also facilitating supervisory requests, such as supervisory stress testing. Use of artificial intelligence, advanced data analytics, and other emerging technologies could improve firms' ability to provide coherent and timely risk data.

28 "Artificial intelligence" can be defined as an entity (or collective set of cooperative entities) that is able to receive inputs from the environment, interpret, and learn from such inputs through advanced data-analysis techniques that aim to mimick the cognitive functions of the human mind (for example, deducing facts, reasoning, creative problem-solving for issues, representing knowledge, planning and social intelligence), and to perform behaviors and actions that help the entity achieve a particular goal or objective over a period of time. "Machine learning" is the science of getting computers to learn and improve their learning over time in autonomous fashion, by feeding them data and information in the form of observations and real-world interactions.

29 Initiatives in a number of countries involving the use of innovative technologies for ID services are in different stages of development. For example, in the United Kingdom, the government is promoting e-identification through its Verify program, to which banks such as Barclays contribute by certifying the identity of their customers. In Canada, SecureKey, a private-sector company that includes a number of banks as investors, proposes to use a third-party blockchain as an identity and authentication provider to simplify consumer access to online services and applications. Similarly, in the Netherlands a service called IDIN, supported by seven Dutch banks, was launched in 2016 to enable customers to identify themselves to other organizations online using bank authentication credentials. Both the UK and Canadian initiatives are supported, to some degree, by governments. In these identity "ecosystems," banks may provide identity information, subject to customer consent, as well as receive it.

30 Initially, new providers entered the market for payment services, most notably in the international remittances market. Indeed, the development of non-bank networks to provide cross-border remittances has been one of the most disruptive recent events in the retail payments space, creating so much change in the payments industry as to lead regulators to start regarding the provision of payment services as an autonomous activity, separate from (though often ancillary to) banking services. The social function of remittances, especially cross-border remittances—that is, facilitating repatriation of salaries of foreign workers—{-OK?-}became the major focal point of debate, especially when it was clear that in some countries revenues from these transfers covered a high quota of domestic income. See World Bank (2012).

31 The United Kingdom has been a pioneer since the launch of Faster Payments Service in 2008. National regulatory authorities there have been very active through multiple initiatives, including the Competition and Markets Authority's open banking, the Financial Conduct Authority's new credit card rules, and the regulatory sandbox initiative. Further, initiatives such as the New Payments System Operator are driving industry uptake of innovations such as open banking. In the United States, regulators are focusing on standardization and risk-reduction initiatives, and the country has advanced standards and rules in areas such as AML and financial stability. With new initiatives to grant banking licenses to fintechs, the rollout of the Clearing House's real-time payments, and further uptake of open banking, the United States may soon move ahead with the help of a more balanced and collaborative approach by regulators and other industry stakeholders. Some of the reactive countries, such as Brazil and Thailand, have conservative regulators that have initiated few or no forward-looking initiatives and have reluctant demand-side institutions; other countries such as Singapore, Australia, and Sweden are more proactive and open to initiatives in the areas of digital payments (including cash-use reduction and contactless cards), virtual bank licenses, fintech-development programs, and open banking activities. Asia Pacific is witnessing much traction in regulatory activity, and regulators are adapting ideas from elsewhere. In particular, India is forging ahead of its peers, and initiatives such as open banking, P2P lending, and demonetization are taking hold.

32 In this area, particularly innovative from the regulatory perspective has been the European Union's Directive (EU) 2015/2366, also known as Payment Services Directive 2 (PSD2), to regulate payment services and PSPs throughout the European Union and European Economic Area. PSD2 mandates open access to certain types of customers' banking

data for non-bank licensed providers of payment-initiation services and account information services. This data consists of designated payment account-related data and the associated payment transactions. Providers are thus allowed to acquire information pertaining to personal online banking accounts, if customers explicitly so choose, and banks are not entitled to deny their access right. Under PSD2, customers should be able to open one app for one account and see a list of all their accounts, even those with other banks; authorize licensed third parties to access a certain set of their payment-related banking details without having to provide log-in details; and decide which information they want to share with what provider and for how long. The owner of the information is the consumer, and the account data are portable. Thus, if the client grants access to this information by other third-party service providers—for example, an application to display aggregate information on the client's payment accounts—the bank may not refuse the service provider access to that data.

33 In other jurisdictions, comparable developments include the revisions to the Banking Act of Japan in 2017, which included provisions to encourage banks to open their APIs, as well as banks' ability to acquire fintech firms and/or collaborate with them to promote innovation and efficiencies. The Canadian competition authorities in 2017 also completed a similar review of the payments sector (along with a review of lending and equity crowdfunding, and investment dealing and advice). The recently passed Mexican Fintech Law (approved on March 1, 2018) includes requirements for fintech firms and novel models (such as regulatory sandboxes) to open data through APIs to third parties and allows them to collect fees. To prevent these fees from being excessive or incongruent, financial authorities will authorize the proposed fees and can veto them. In Australia, the government has announced a "consumer data right" (giving customers a right to direct that their data be shared with others they trust) that will be applied sector by sector, with open banking to be the first application. Other countries that have passed open banking regulations include Honk Kong, India, Singapore, and the United States.

34 This has been the case particularly in Europe with the General Data Protection Regulation (GDPR) and the ePrivacy Regulations (ePR). Other countries, such as Canada, Japan, and Israel, are working toward data-privacy and protection laws that are on par with GDPR and ePR standards. The GDPR primarily aims to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the European Union. The regulation clarifies the rights of customers (data subjects) and defines different data types, setting out the legal obligations of data controllers, data processors, and data subprocessors when interacting with data subjects and with each other. The regulation represents the most significant change in the payments environment in terms of risks to merchants (data controllers) and entities supporting data processing (data processors and subprocessors). It puts the rights of the data subjects above all others, legally obliging both data controllers and data processors to put the interests of the data subjects above their own. The European Union's new payment regulation PSD2 is wholly dependent on the GDPR to establish firmly the legal rights of the data subject and the legal obligations of the data controller and processor in order to support the framework it sets to secure transactions between merchants and their customers. The European Union's ePR broadens the scope of the current ePrivacy Directive and aligns the various online privacy rules that exist across European Union member states. The ePR takes on board all definitions of privacy and data that were introduced within the GDPR and acts to clarify and enhance it. The ePR specifically covers the areas of unsolicited marketing, cookies, and confidentiality.

35 Youth unemployment rates in the region have been the highest in the world for over 25 years, reaching 30 percent in 2017. Only in Qatar is the youth unemployment rate lower than the world average, due to the country's capacity to absorb young nationals into public-sector jobs. By 2020, more than 60 million jobs need to be created in order to absorb entrants to the job market and stabilize youth unemployment (UNDP 2016)

36 In the Gulf Cooperation Council countries, informality is low partly because of its heavy reliance on documented foreign workers and government employment.

37 The percentage of respondents who report having an account (by themselves or together with someone else) at a bank or another type of financial institution or report personally using a mobile-money service in the past 12 months.

38 See IMF (2018, 2019) and IMF-World Bank (2019).

39 For a comprehensive a detailed technical illustration of DPS and their evolution, see ITU (2017f).

40 In Kuwait, for instance, One Pay and Quickpay enable customers to pay for their bills (including rent, pay-TV subscriptions, school fees, and international payments) from a dedicated mobile application, and in 2017 Kuwait Finance House launched its KFH Wallet, which allows users to perform mobile payments at merchants' NFC-enabled POS terminals in the country. Furthermore, the National Bank of Kuwait made its contactless payment service NBK Tap & Pay available in 2018 on customers' wristbands. The United Arab Emirates (UAE) is another country that has experienced dramatic growth in the number of available m-payment services. Mobile operator Etisalat, for instance, launched its mobile wallet, Etisalat Wallet, in 2016. That year Emirates NBD released NBD Pay, a contactless payment service enabling purchases at NFC-compatible POS terminals. Platforms such as Samsung Pay and Apple Pay already operate in the UAE. In addition, a consortium of 16 banks in the UAE is working on launching the EDW (Emirates Digital Wallet), which offers a multitude of m-payment services, such as m-POS payments and m-P2P bank payments.

41 Start-ups operate in the lending business (including crowdfunding, capital-raising solutions, money circle, peer-lending, and loan-comparison platforms) as well as in the area of mobile and online payments, international money transfers, wealth management, digital wallets, insurance services, and blockchain-based solutions such as cryptocurrencies.

42 Green shoots include Bahrain-based PayTabs and Jordan-based ProgressSoft and eFAWATEERcom, which provide digital payment solutions for banks and small and medium-size enterprises. UAE-based Beehive and Eureeca, Lebanon-based Zoomaal, and Jordan-based Liwwa provide crowdfunding and peer-to-peer lending in the region.

43 Some of the major deals that took place in 2017 included a $20 million investment in PayTabs, a $3.5 million investment in YallaCompare, and a $1.46 million investment in Now Money. In addition to these deals, TPay, the MENA region's first and largest direct carrier-billing platform, acquired its competitor and the second largest direct carrier-billing service provider in Egypt, DCBEgypt, for an undisclosed amount.

44 The data from figure 10 shows that the MENA region's digital payments average (non-high-income) in 2017 is lower than all regional averages (non-high-income) except that of South Asia. As regards bank account transactions, the MENA region (not excluding high income) had a lower average than all other regions (not excluding high income) but Sub-Saharan Africa.

45 Yemen is, indeed, a unique case, in that women do not seem to have made any digital payment, and the 1 percentage point is attributed entirely to men.

46 Given the conflicts in Syria and Libya, no information about functional payment systems is available for these countries.

47 This is consistent with the findings of the World Bank's forthcoming *MENA Flagship Report, 2020*, from D. Lederman and R. Cull.

48 By comparison, Western Europe has achieved 83 percent of its potential vis-à-vis the United States. The analysis is by McKinsey Global Institute (2016a), and the metric of captured digital potential by country is calculated using the McKinsey Digitization Index, which takes digitization in the information and communications technology sector of the United States as the 100 percent frontier base.

49 There is an emerging trend now in the rural areas of emerging economies, where connectivity is being brought to them via Internet balloons, an innovative, cost-effective, and quicker option. These balloons travel on the edge of space, delivering connectivity to people in unserved and underserved communities around the world. These hovering balloons function like a stationary power station that provides electrical connectivity to an area.

50 In developing the building blocks of the strategy framework (see section IV.B), this report has benefitted from the World Bank's research and policy works produced by the Payment Systems Development

Group and from the extensive work done by the International Telecommunication Union (ITU) on digital financial services, including ITU (2017c) and the ITU reports specifically referenced, where appropriate, across the text. Especially insofar as the framework's building blocks deal with the increased use of DPS in relation to financial-inclusion objectives, the report has benefitted from the following important sources: CPMI-World Bank Group (2016); GPFI (2016); ITU (2016a); and the World Bank Development Research Group, Better Than Cash Alliance, and Bill and Melinda Gates Foundation (2014).

51 See G7 France (2019) and Helms (2019). See also World Bank Group (2017) and CPMI (2017).

52 While "fintech" refers to a financial institution that applies new technologies to deliver new or better financial services (a traditional bank offering mobile banking service is a good example), "techfin" refers to a technology firm that wants to deliver financial products on the basis of existing tech solutions. Examples of techfin institutions include Google, Amazon, Facebook, and Apple in the United States, and Baidu, Alibaba, and Tencent in China. These are also usually large fintechs or "bigtechs." Like the fintechs, these companies offer specific financial products and services, unbundled from the banks' value chain but nevertheless incorporated within their own value proposition. A common aspect of the general strategy employed by such companies is building around their customers an ecosystem of products and services (social media, e-commerce, search engines, operating systems, app stores, and so on) that are interconnected between them.

53 In 2018, the International Monetary Fund and World Bank Group launched the *Bali Fintech Agenda*, a set of 12 policy elements aimed at helping member countries to harness the benefits and opportunities of rapid advances in financial technology that are transforming the provision of banking services while at the same time managing the inherent risks (IMF 2018). The agenda proposes a framework of high-level issues that countries should consider in their own domestic policy discussions and aims to guide staff from the two institutions in their own work and dialogue with national authorities. The 12 elements were distilled from members' own experiences and cover topics relating broadly to enabling fintech, ensuring financial-sector resilience, addressing risks, and promoting international cooperation.

54 Microfinance clients should be encouraged to accept digital payments in their own businesses. Microfinance institutions should consider launching incentive programs supporting their clients in accepting cashless payments in the course of income-generating activities for which a microfinance loan has been provided. They should also provide technical assistance and support their clients in educating them about cashless payment methods and delivering hands-on help when registering as merchants with financial institutions.

55 Electronic money (e-money) is defined as monetary value that is (i) made available to users to conduct transactions through an electronic device; (ii) accepted as a means of payment by parties other than the issuer; (iii) issued against receipt of funds in an amount equal to the monetary value made available; (iv) electronically recorded; (v) denominated in the same currency as the fiat money that backs it up; (vi) mirrored by the value stored in one or more accounts usually open in one or more bank(s); and (vii) redeemable for cash or deposits on demand. Examples are debit or prepaid cards and mobile money. Note that the terms *electronic* and *digital* as they apply to money are not interchangeable; the word *digital* refers to the broader category of representations of value that exist only in electronic form and are not tangible and include (besides e-money) monetary values that are not backed by fiat money and are not denominated in the same currency as fiat money. An example is Bitcoin.

56 For a discussion of the alternative policy options, see GSMA (2016b).

57 E-money funds are subject to some of the same types of risk as traditional sight deposits, including the risk that the payment service provider (PSP) or an employee of the PSP misuses or absconds with the funds, that the PSP faces bankruptcy, or that the financial institution that holds the underlying funds (but is not the actual PSP operating the e-money accounts) faces bankruptcy. Furthermore, e-money transaction accounts differ fundamentally from deposit transaction accounts in that e-money accounts are not designed to facilitate financial intermediation. In this context, clarity regarding the potential use of funds held in e-money accounts becomes important. Thus, unlike deposit transaction accounts, whose providers are subject to strict banking supervision, onlending e-money funds (or investing those funds) by the PSP would normally constitute fund misuse.

58 In general, deposit insurance schemes do not cover e-money accounts. In at least one case, though, protection is available through "pass-through" deposit insurance. Under this scheme, the deposit insurance on the bank account in which the underlying customer funds are held by the PSP passes through to the e-money account holders. (See CPMI-World Bank Group 2016.) For a discussion of the options available to insure the funds underlying e-money, see di Castri (2013).

59 On this issue, see Bossone (2017).

60 As defined by the Organisation for Economic Co-operation and Development (2017), big data is commonly understood as "the use of large-scale computing power and technologically advanced software in order to collect, process and analyze data characterized by a large volume, velocity, variety and value." Consumer data stemming from online behavior, geolocation tools, digital payments, and wearables is fueling a gold rush in several industries worldwide and affecting consumer's daily financial lives in terms of product choice as well as privacy and data protection.

61 A strong appeal for fintechs in the payments business originates from the opportunity to collect and analyze customer data. Payment activities are literally where the money is; knowing how consumers spend their money represent potential profit pools to companies. Consider Southeast Asia as an example. Start-ups have already amassed more data on Southeast Asian citizens and their habits than any census could possibly provide because they offer convenient services for free or at a nominal fee. As competition for markets and customers reaches a stalemate, Southeast Asian unicorns—such as Grab, Go-Jek, Razor, and Sea—have expanded their payment options and absorbed fintech companies, specifically payments companies. This is because every service ends with a transaction and broadens the amount of information that can be collected. For example, Go-Jek and Grab can now paint a vivid picture of users' movements, schedules, and even financial habits. This opens doors for new products and services: Grab plans to use information collected through their fintech products to create alternative credit ratings, which could then be tied to banking products, while Go-Jek has made the leap into credit through its partner Findaya, which has started testing a credit option that allows users to repay at a later date. Venturing into fintech also positions companies to expand their understanding of customers and improve their non-financial products and services, and tech companies that go into finance can open up new revenue streams by selling information to third parties. Even if start-ups have a niche or small group of customers, the data will be valuable to other players in the market.

62 For a discussion of how big data is used in payment systems and how to make sure it works for everyone, see PSR (2018). For a discussion of big data implications for competition policy, see OECD (2016).

63 In a market economy, private-sector PSPs seek to maximize their profit and may therefore focus on those geographic areas and customer segments that promise to yield the largest margins and neglect the less promising ones. In several countries, post offices have traditionally offered certain financial services and rely on very large branch networks that can be used for financial-inclusion purposes. Also, in the attempt to expand access to payment services cost effectively, bank and non-bank PSPs use local entities, such as small shops, as agents to provide basic payment and banking services on their behalf. Interoperability between access points enhances considerably their potential to service the national payment system and their contribution to financial inclusion.

64 Power-supply interruptions harm PSPs, users, and access points, and the geographic areas with the highest rate of financial exclusion are usually those with no reliable access to electricity. Lack of a regular power supply, especially in remote places, is one of the reasons that PSPs cite most often for not deploying ATMs more widely. Today, vendors offer solutions that minimize the impact of power outages on ATMs and POS terminals. Many companies are working on products based on kinetic or solar energy. Solutions are becoming available for charging phones conveniently and at low costs. See, for instance,

BusinessTech (2014), Jetley (2014), and Vortex (http://www.vortexindia.co.in).

65 For an extensive treatment of access points, see CPMI-World Bank Group (2016).

66 For a discussion of communication technology delivery channels, see ITU (2016d).

67 Interoperability in DPS can take place at different levels. It can occur (i) at the mobile network level, with customers being able to access their mobile money through different SIM cards; (ii) at the agent level, as in the case of Kenya (no agent exclusivity); or (iii) at the digital platform level, where payment services take place either on net or off net. In the latter case, it is critical that regulatory safeguards are in place to avoid discrimination between on- and off-net traffic, which is beneficial to the incumbents.

68 This is to be distinguished from sharing of agents (whereby an agent may perform cash-in and cash-out transactions for multiple PSPs) and from network neutrality (whereby customers can access the same mobile financial services through different mobile network operators, or MNOs).

69 Interoperability is also important for financial-inclusion purposes. The economics of reaching rural customers makes it unrealistic for all PSPs to set up agents in all geographic areas; at the same time, national authorities want to ensure some level of basic and convenient service provision and customer choice in payment services everywhere in their country. One means of achieving this goal is to promote interoperability of PSPs, so that customers can interact with other customers or merchants that they need to reach without being required to open multiple accounts.

70 Lack of account-to-account interoperability in e-money causes inconvenience, cost, and inflexibility for users. Recipient cannot receive the money in their mobile wallet and can obtain the funds only by physical withdrawal from the sending provider's agent (when this has sufficient cash). Also, additional charges may apply to senders for such transfers and to recipients for cash withdrawals—charges that would not apply in account-to-account transfers. Finally, these services are usually unavailable for transfer values below a certain value, making it less convenient than transferring between electronic wallets. These factors make it far more desirable for senders and recipients to hold accounts with the same provider, typically the leading one (which may be one reason why many subscribers in countries with significant mobile-money businesses will hold more than one subscription).

71 Providers with a smaller customer base may be prevented from competing by certain pricing strategies of those with a larger customer base. Large providers may exploit network effects to preserve and deepen their market power by using low on-net prices and higher off-net prices. This may make it significantly more expensive for their customers to transact with customers on other networks than to transact on the same network. This makes the larger providers more attractive for customers, and where the larger providers are dominant, a large price differential between off-net and on-net transaction can harm competition.

72 An example of industry-led mobile-money interoperability, albeit limited, comes from Tanzania, where the four leading MNOs, supported by the International Finance Corporation (IFC), worked together over the course of a year to agree on payment-scheme rules, including exchange fees and dispute resolution, among others. The Bank of Tanzania supported the discussions and was kept informed on how the discussions were proceeding, so that by the time an agreement was finalized, all parties involved, including the regulator, were fully informed and in support of the arrangement. Another example that comes from Africa is that of Mowali, a joint venture of Orange Group and MTN Group (two of Africa's largest mobile-money providers) launched in early 2019 to enable interoperable payments across the African continent. Mowali is available to any mobile-money provider in Africa. Zelle, a P2P mobile payments network in the United States, is another example of a private sector–led interoperability initiative. While not all banks are on board, a considerable number are already using it, and when all banks adopt it, Zelle will be the only fully interoperable P2P mobile payments network in the country that allows individuals to send/receive mobile payments seamlessly in real time.

73 For a discussion of the right timing for and scope of the regulator's actions to induce interoperability, see ITU (2016a).

74 The cases of Kenya and Tanzania are paradigmatic in this regard: in Kenya, the Competition Authority ordered Safaricom to open up its network of agents to rival firms; in Tanzania, on the other hand, three operators entered into an operability agreement, while Vodacom, the largest operator, refused to be a party to the agreement. See Bourreau and Valletti (2015).

75 A fast payment is a payment in which the transmission of the payment message and the availability of "final" funds to the payee occur in real time or nearly real time on as close to a 24/7 basis (24 hours a day, 7 days a week) as possible (CPMI 2016).

76 The expression "customer due diligence" (CDD) is often used interchangeably with the expression "know your customer."

77 In 2015, Tanzania established its own tiered CDD regime for mobile money, encompassing three tiers: Tier 1, for basic electronically registered accounts, requiring only a registered phone number; Tier 2, requiring both a registered phone number and in-person confirmation and a copy of an acceptable national ID document; and Tier 3, which is aimed at small and medium-size enterprises and includes not just the full CDD of Tier 2 but also tax ID and VAT registration numbers along with business license numbers. While the new system is considered a good approach for expanding mobile money, the Tanzanian banking sector continues to operate under its traditional, more stringent CDD requirements.

78 A KYC registry is a centralized repository for maintaining customers' KYC records. The registry involves a due-diligence process to obtain the information of the customer (that is, the identity and the address) and stores the information in a digitally secure electronic format. The registry then provides for an advanced and secure user-authentication mechanism for system access. The registry employs uniform KYC norms and interusability of the KYC records among various concerned stakeholders. A KYC registry reduces the hassle of providing a customer's KYC documents repeatedly and getting them verified each and every time a customer builds relationship with a financial entity. India's Central KYC is an example of a centralized KYC registry. Recently, SWIFT worked with the world's largest correspondent banks to define a set of data and documentation that addresses KYC requirements across multiple jurisdictions and offers its clients centralized KYC registry services. The information collected and shared through the registry includes, among other things, customer identification, ownership and management structure, types of business and client base, operating geographies, compliance information, and tax information. The registry prompts data contributors to upload the required documents. Once submitted, the data are thoroughly cross-checked and reviewed by SWIFT. The information that is then made available to clients is standardized, comparable, and reliable.

79 The standards and practices should include, among others, measures to strengthen authentication mechanisms to demonstrate ownership of the devices, to ensure that regular security updates are pushed to devices, and to facilitate easy access of users to security patches; to make sure that device manufacturers and network operators configure operating systems in ways that reduce the attack surfaces; and to ensure that applications are based on state-of-the-art encryption, authenticated communication, and secure coding technologies. Also, network operators should be required to implement security policies that maintain the integrity of their networks and prevent unauthorized access to customer accounts.

80 The European Central Bank has developed cyber resilience oversight expectations to provide financial market infrastructures (FMIs) with detailed instruction on how to operationalize the CPMI-IOSCO guidance, to provides overseers with clear expectations to assess the FMIs for which they are responsible, and to provide the basis for a meaningful discussion between the FMIs and their overseers (ECB 2018). Interestingly, since the cyber-threat landscape is constantly evolving and reaching higher levels of sophistication, the expectations set out levels that provide the overseers and FMIs with a benchmark against which they can evaluate the FMIs' current level of cyber resilience, measure progress, and establish priority areas for improvement. The expectations establish three levels: evolving, advancing, and innovating.

81 For a comprehensive analysis of competition and related policy aspects in the retail banking markets, see World Bank (2020a).

82 Appendices D and E discuss barriers to entry and the risks of market foreclosures to fintech operators typically found in DPS markets.

83 Examples of jurisdictions that still adopt bank-led models for the provision of e-money services are Bangladesh, Egypt, Ethiopia, Pakistan, and Uganda. India, too, originally took a bank-led approach, but in 2015 the authorities allowed new institutions (called "payments banks") to offer basic payments and savings services—including issuing e-money and providing e-money services—to low-income customers in a more cost-efficient way than commercial banks. As limited-purpose banks, payment banks are subject to lower prudential requirements than commercial banks but are barred from extending credit. Many of these banks are owned by a range of non-bank entities with prior experience in payment services, such as MNOs, the India Post, agent companies, and prepaid payment issuers.

84 Regulators may face challenging issues in working out what is innovation and investment and what is actually anticompetitive (discriminatory or exclusionary) behavior, and whether to intervene or hope the market will resolve matters by itself. In Kenya, Safaricom, operating the M-Pesa payment system, resisted the entry of competing service providers, and Egypt is currently wrestling with interoperability issues, including integrating a mobile payments gateway into the EG-ACH (Egyptian Automated Clearing House). The EG-ACH is governed by the Egyptian Banks Company under the supervision of the Central Bank of Egypt. These are just two of many examples from many countries.

85 A mobile-money provider that is not able to obtain access to the network channels directly from the MNO might seek to use an aggregator that can provide it with access to several MNOs, possibly on better terms because the MNO may not initially be aware that the mobile-money provider is behind the aggregator. However, this strategy may not succeed where the MNO learns that the aggregator is making network access available to the competing mobile-money provider. In some cases, MNOs have even threatened the aggregator with cutting off network access if it finds the aggregator is supplying a competing mobile-money provider. ITU (2016d) reports an illustrative example from Uganda.

86 See Gupta (2015).

87 The three systems support UK retail payment services: Bacs provides direct debit, direct credit, and check-clearing services. Faster payments service provides nearly real-time payments, one-off forward-dated payments, and standing orders. LINK enables payment account holders to take cash out (among other activities) using the LINK network of ATMs.

88 In the case of USSD (Unstructured Supplementary Service Data), the most commonly used channel, MNOs may charge the mobile-money provider and the customer nothing for a USSD session, which is more likely if the payment service is provided under a partnership between the MNO and the provider. See footnote 118. In other cases, the MNO may charge the customer, in which case the charge (although paid by the customer) is usually negotiated between the MNO and the provider, or the MNO may charge the customer nothing but charge the provider a negotiated price. The provider, in turn, may pass the charge on to the customer or absorb it so as not to discourage the customer from using the service.

89 The ability of network operators to practice anticompetitive pricing should diminish as smartphone penetration and literacy rise, mobile data services are available, prices fall, and new applications are developed. Customers will be able to access mobile-money providers directly over the Internet, and providers will be able to connect with them directly, rather than acquiring a dedicated link using USSD channels or STK-based interfaces. STK (Systems Tool Kit) is a software package that allows engineers and scientists to perform complex analyses of ground, sea, air, and space assets and share results in one integrated solution.

90 See, for example, GSMA (2015, 2016c).

91 See, for instance, the memorandum of understanding between the Competition and Markets Authority and the Office of Communications in the United Kingdom. Framed in the context of the Enterprise and Regulatory Reform Act of 2013, the memorandum governs the concurrent competition powers of the two agencies. More broadly, the Competition and Markets Authority and the sectoral regulators have committed to using concurrent powers through the establishment of the UK Competition Network, which represents an enhanced forum for cooperation that enables closer working with the objective of more consistent and effective use of competition powers across all sectors, with a view to promoting competition for the benefit of consumers and to preventing anticompetitive behavior both through facilitating the use of competition powers and developing pro-competitive regulatory frameworks.

92 A relevant example is the financial regulatory provisions for PSPs, which also regulate the access by PSPs to the data stored by established financial institutions (for example, the banks where the clients have their current account and mortgage loan and receive their salary payments). The rules to ensure access to customers' payment data to third-party PSPs are critical for competition, and competition law instruments can be a useful mechanism to foster compliance with regulatory rules. However, the rules themselves exceed the scope of competition policy.

93 See, for instance, Ahrend, Arnold, and Murtin (2009); Fisher and Grout (2017); Vives (2016); and Maes and Kiljanski (2009).

94 Regulators should require PSPs to (i) set clear, simple, and comparable disclosures of terms, fees, and commissions; (ii) issue periodic account statements showing transactions and fees; (iii) advertise toll-free customer hotlines; (iv) set up procedures and responsibility for unauthorized or mistaken transactions and system outages; (v) establish responsible and fair-lending and debt-collection practices; (vi) issue consumer guidance about how to use a DPS as well as security safeguards to protect against unauthorized use, disclosure, modification, and destruction of personal data; and (vii) provide government contact details for consumer queries (such as phone numbers and websites). All consumer information should be provided digitally (including over a mobile phone) and retained.

95 As the provision of DPS entails risks, regulations and policies should induce PSPs to manage and mitigate these risks. Risk-management requirements and policy expectations relate to the oversight role that the public authorities (typically, the central banks) play in the context of DPS ecosystems. Oversight of DPS will be discussed in section IV.C.

96 For example, some mobile-money providers do not clearly disclose the amount of the fee associated with a transfer, the interest rate applicable to a loan, or the USSD charge the customer may be paying for the transaction, or some providers disclose prices only after the customer has contracted for the service.

97 The GDPR, discussed earlier, applies to the processing of personal data of data subjects in the European Union, regardless of the location of the data controller and/or of the data processor. It clarifies the concept of personal data. Importantly, it strengthens the obligations imposed on organizations, such as the appointment of "data-protection officers," performance of "privacy impact assessments," adoption of security and data-protection policies and procedures, as well as the obligation to notify the competent authorities and, in certain cases, the data subjects of data breaches. Further, it defines more demanding requirements regarding the information to be provided to the data subject as well as the data subject's consent and includes the right to be forgotten. It also establishes rules on profiling and authorizes very substantial fines for non-compliance.

98 The term "financial literacy" is here defined as in OECD/INFE (2012)—that is, "a combination of financial awareness, knowledge, skills, attitude and behaviours necessary to make sound financial decisions and ultimately achieve individual financial wellbeing."

99 For example, regulators and the industry should undertake active customer-awareness campaigns to educate consumers about malicious messages, phishing, and spoofing attacks, and they should encourage consumers and victims of attacks to report malicious attackers to the providers. This would allow providers to send warning messages throughout their network, ensure that attackers are permanently blocked from the system, and provide a means of investigating and prosecuting the perpetrators of these actions.

100 The oversight of payment and settlement systems is typically "a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assess-

ing them against these objectives and, where necessary, inducing change" (CPSS 2005, 1). Through oversight, the central bank ensures that such systems (i) operate smoothly, efficiently, fairly, and transparently for all participants and users; (ii) are robust against the risk of transmitting shocks through the economy because of an individual participant's failure to meet its payment obligations; (iii) continue to operate even in the event of major disruptions to systems or providers; (iv) continually evolve and achieve the level of technological and institutional development necessary to satisfy the payment needs of a growing, open, regional, and internationally integrated economy; and (v) deliver safe and cost-effective payment products and services to users and facilitate financial inclusion. In the case of retail payment services (including as such also the DPS), however, certain jurisdictions assign regulatory, oversight, and supervisory powers to agencies other than the central bank, leaving to the latter the responsibility for the oversight of only risks and issues of systemic nature. Canada and the United Kingdom are relevant examples. The report refers interchangeably to "DPS overseer" or simply "overseer" whether the function is a responsibility of the central bank or any other agency.

101 The World Bank will soon publish *Towards{-Toward?-} More Effective Oversight and Settlement Systems and Services: A Handbook* (the Oversight Handbook), a policy research work that examines all relevant aspects of payment-system oversight based on international experience, covering topics from general concepts and principles to operational applications. The Oversight Handbook will provide a toolkit for central banks and for the World Bank's technical assistance projects. Standards for the oversight of interoperable arrangements have been developed by the International Telecommunication Union (2016b, 2016c).

102 Overseers should have in place appropriate monitoring measures to hold PSPs accountable for their performance and compliance with rules. These should include standardized as well as ad hoc reporting requirements covering all relevant aspects of their activities and market conduct.

103 In the context of country-specific technical assistance programs, the World Bank develops templates and tools for the oversight and supervision of PSPs and instruments (which include DPS and DPS providers).

104 With regard to fintech firms, a working group on fintech data issues was set up by the IFC to take stock of existing data sources, identify data gaps, provide guidance on fintech classification issues, and develop a way forward. In addition, the IFC conducted a membership survey in 2019 that informs about approaches that central banks pursue with regard to fintech data. The survey covers the current statistical infrastructure, "fintech gaps" in statistics, fintech data demands from a user perspective, ongoing initiatives to measure fintech, and the role of international coordination. One of the main issues is that there is no clear definition of what "fintech" actually means. The Financial Stability Board defines fintech as a technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on the provision of financial services. This definition does not match easily with existing statistical concepts, and official data are often lacking. A review of statistical classification systems such as the Central Product Classification for products and the International Standard Industrial Classification of All Economic Activities shows that defining fintech firms from a statistical point of view is challenging. Fintechs are currently in a state of limbo with regard to classification, as they do not (yet) have a position in statistical classification systems. The IFC membership survey's preliminary results suggest that this is one of the most important issues. For all definitions currently in use, including the Financial Stability Board's definition cited above, the two descriptors "innovative" and "technology" are essential. These concepts are not time invariant. Thus, a firm that is labeled "fintech" today may not be a fintech 10 years from now even if it continues to provide the same services, mainly because the technology will no longer be "new." One may be able to distinguish between fintechs and other providers of financial or non-financial services, given the current state of financial technology, but these distinctions will not lead to partitions that are stable over time, in the way required for the purposes of statistical classification. Fintech activities combine both IT-driven business services and financial services. If a fintech company is registered as an IT business, statistics may be missing its financial service activity. This could potentially lead to statistical biases when measuring the size and growth of the financial sector, its value chains, and thus its connectedness. Currently, dynamics in the fintech sector are not being adequately captured by the financial-sector statistics, and data on the use side of fintech by households and firms is also extremely scarce.

105 The notion of "dynamic compliance" refers to automating the regulatory compliance processes by continuously assessing whether the data reported are accurate and relevant and by embedding rules into IT protocols to eliminate chances of non-compliance.

106 A "data warehouse" is a database that is designed for query and analysis, rather than for transaction processing. It usually contains historical data derived from transaction data, but it can include data from other sources.

107 Owing to the key role of telecommunications in the provision of digital services, the institutional framework for the oversight of DPS provision should be designed to accommodate cooperation between the central bank, as overseer of the national payment system, and the telecom authority that is responsible for regulating DPS providers as telecommunication operators. The establishment of inter-institutional cooperation agreements (for instance, in the form of a memorandum of understanding) helps both to frame the mutual responsibilities of the agencies involved and to identify the various areas, activities, and tasks to articulate their cooperation. See below in the main text.

108 Examples of how authorities cooperate in a variety of contexts, and the challenges they encounter in undertaking cooperation, are described in CPMI-IOSCO (2019).

109 Cooperative arrangements between authorities should in no way prejudice the statutory or legal or other powers of each participating authority, nor should these arrangements constrain in any way an authority's powers to fulfill its statutory or legislative mandate or its discretion to act in accordance with those powers.

110 In the context of country-specific technical assistance programs, the World Bank Group assists the national authorities of its client countries in setting up inter-institution memorandums of understanding.

111 A good example of payment-system policy making driven by policy dialogue is PSR (2015).

112 See the *Toolbox for Assessing Digital Finance Development in World Bank Member Countries* (World Bank Group 2018b) and *Digital Economy for Africa* (World Bank Group 2018a).

113 The World Bank is developing the policy concept note *Toward Digital Government Payment Programs: A Strategic Framework*, which will be made available soon for national policy authorities in the context of technical assistance programs in this area.

114 USSD is a Global System for Mobile (GSM) communication technology that is used to send text between a mobile phone and an application program in the network. Applications may include prepaid roaming or mobile chatting. USSD is similar to Short Messaging Service (SMS), but, unlike SMS, USSD transactions occur during the session only. With SMS, messages can be sent to a mobile phone and stored for several days if the phone is not activated or within range.

115 India has recognized the key role that merchant acceptance will play in creating a cashless economy. However, small corner stores, which many Indians rely on to make their daily purchases, cannot afford the installation or maintenance of full-fledged POS terminals. As a result, connecting merchants to acceptance networks through a QR code–based standard has become the logical solution. International card networks, such as Visa and Mastercard, enthusiastically embraced the technology. However, maintaining separate QR code standards for each network, without interoperability arrangements, could diminish potential gains, and forcing merchants to display three or more different codes—one for each scheme—would create confusion among them and their customers. Consequently, the National Payments Corporation of India worked with the largest networks to create Bharat QR, an interoperable standard for QR code–based merchant payments, which has subsequently inspired the creation of a global standard for QR code–based payments, developed by the EMV consortium and adopted by payments regulators across the world, including the Central Bank of Egypt. In addition to the development of an interoperable QR code technology, India has provided economic incentives for acceptance of digital payments by smaller merchants: the central bank has decided to cap the merchant discount rate for small businesses,

while the government has committed to covering the cost of the merchant discount rate for small transactions (not exceeding Rs 2,000) for the period of two years.

116 This subsection draws on Klapper (2016).

117 Globally, 585 million women pay for utilities in cash, while 225 million women do the same for school fees. Paying these expenses digitally could save women untold time and resources. Working women in developing countries often have to miss work and pay transportation fees to pay their children's school fees, resulting in wage and income losses.

118 In Bangladesh, IFC surveys found that, although 52 percent of female customers preferred female agents, 97 percent were using male agents due to female agent scarcity. Women who visited female agents reported a higher median number of transactions than those who visited male agents (IFC 2018a).

119 In Togo, where 62 percent of women and 47 percent of men lack an account, 30 percent of financially excluded people cite lack of identification as one of the reasons they do not have an account, according to the 2017 Findex data.

120 The International Labour Organization identifies a list of essential services (ILO 2006).{-YEAR OK?-} These services are those that, if not provided, would endanger life, personal safety, and health of the whole or part of the population. During the COVID-19 outbreak, many countries imposed restrictions to people's movements or outright curfews on parts or all of the population, with certain allowances for the following essential services: food, medicine and healthcare, electricity, water and telecommunications, banking, public safety (police, firefighters, armed forces, prison services), basic transportation, postal services, and garbage collection. In some countries, there are strict curfews for older residents, restricting their movements even for the purpose of accessing essential services.

121 The document under elaboration, "Impact on Payment and Settlement Systems—COVID Response Note," covers other issues such as the adequacy of critical payment systems and PSPs' business-continuity plans, liquidity support to PSPs, and provision of cash services (World Bank 2020b).

122 In a recent three-part column, Bossone and Natarajan (2020a, b, c) {-SOURCES NOT IN REFERENCES-} discuss how governments can get funds to people and businesses in need and enable access to money during emergencies like COVID-19 and the assistance provided by the World Bank Group to its client countries in this context. The first part identifies the challenges affecting payment services during emergencies and discusses measures to ensure that payment systems keep operating. The second part discusses the special role that government payments and international remittances play, in particular for developing economies, and identifies measures to ensure their accessibility and resilience, especially in times of emergencies. The third part analyses the role that a central bank digital currency can play in this context and outlines the key steps required for its successful implementation and proposes improvements to the existing payments infrastructure to ensure continued operability, especially in times of emergencies.

123 This appendix draws on Autoridade da Concorrência (2018).

124 This appendix draws on Autoridade da Concorrência (2018).

125 See https://app.parr-global.com/intelligence/view/prime-2608780.

126 See Bundeskartellamt (2017).

127 See ICA (2017).

128 The decree law entered into force on March 9, 2018.

WORLD BANK GROUP