

IMF Working Paper

Middle East and Central Asia Department

Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions

Prepared by Inutu Lukonga¹

Authorized for distribution by Allison Holland

September 2018

IMF Working Papers describe research in progress by the author(s) and are published to elicit comments and to encourage debate. The views expressed in IMF Working Papers are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

Abstract

Financial technology (fintech) is emerging as an innovative way to achieve financial inclusion and the broader objective of inclusive growth. Thus far, fintech in the MENAP and CCA remains below potential with limited impact on financial inclusion. This paper reviews the fintech landscape in the MENAP and CCA regions, identifies the constraints to the growth of fintech and its contribution to inclusive growth and considers policy options to unlock the potential.

JEL Classification Numbers: E2, G2, N2

Keywords: Fintech, Cyber Risks, Financial Stability, Inclusive Growth and Financial Inclusion

Author's E-Mail Address: ilukonga@imf.org

¹ The author would like to acknowledge the Research support provided by Mr. Sebastian Herradorr, the very helpful discussions held with Messrs. Alice Zanza, Da Silva Pereira Maria Do Ceu, Karol Karpinski, Ahmed Faragallah, and Odinaeva Zarina (All World Bank) and comments from Messrs. Ashraf Khan, Cooper William Allen, Pierre Gaele, Tamas Gaidosch, Masaru Itatani, Saito Masashi, Maria Mendez, Hunter Monroe, Najla Farid Nakhle, Christopher Wilson, Farid Talishli, Hamid Reza Tabarraei (All IMF).

Contents	Page
ABSTRACT _____	1
I. INTRODUCTION _____	1
II. FINTECH: AN OVERVIEW _____	2
III. THE FINTECH LANDSCAPE IN THE MENAP AND CCA REGIONS _____	6
A. Growth Drivers and Prospects _____	11
B. The Legal Framework, Regulation, and Supervision of Fintech _____	14
C. Cyber Risks and Other Vulnerabilities _____	21
D. Factors Impeding Fintech Growth and its Impact on Inclusive Growth _____	25
IV. FINTECH: A VALUE PROPOSITION FOR THE MENAP AND CCA REGIONS _____	31
A. Inclusive Growth _____	31
B. Financial Stability, Integrity and Financial Inclusion _____	36
V. UNLOCKING THE TRANSFORMATIVE POTENTIAL OF FINTECH _____	37
A. Promoting Innovation while Safeguarding Financial Stability _____	37
B. Aligning Fintech with Policy Priorities _____	39
GLOSSARY	
Glossary of Terms _____	44
BOXES	
1. Cross Country Experiences with Fintech _____	41
2. Infrastructure for Digital Financial Inclusion _____	42
3. Cyberattacks Impacting Financial Institutions in MENAP and CCA, 2012-2018 _____	43
FIGURES	
1. Architecture of the Fintech Industry _____	4
2. Enabling Environment for Fintech _____	5
3. Scale of Fintech in the MENAP and CCA regions _____	6
4. Fintech Startups and Investments _____	7
5. Geographical Distribution of Fintech Startups and mobile money services _____	8
6. Fintech Segments _____	9
7. Internet and Mobile Phone Penetration _____	12
8. State of Funding for Startups _____	13
9. Legal Systems in the MENAP and CCA _____	14
10. Countries with Regulatory Sandboxes _____	16
11. Protection of Minority Creditors and Insolvency Regimes _____	18
12. Status of cybercrime legislations in the MENA and CCA _____	19

13. Cyber Security Threats _____	23
14. Key Challenges Facing Fintech Firms _____	25
15. State of the ICT, Payment System and Credit Evaluation Infrastructure _____	28
16. Factors Adversely Impacting the Business Environment _____	29
17. Customer Preferences and Literacy Levels _____	30
18. Unbanked populations and Rural Urban Divide _____	32
19. Unemployment Levels and SME Access to Finance _____	34
20. Displaced Populations and Social Transfers _____	35
21. Remittances Volumes and Transfer Costs _____	36

References _____	45
-------------------------	----

I. INTRODUCTION

Financial technology (fintech) is emerging as an innovative way to achieve financial inclusion and the broader objective of inclusive growth. In addition to improving the speed, convenience, and efficiency of financial services, fintech has potential to promote financial inclusion. More specifically, it can enhance access to affordable financial services for unbanked populations and underserved small and medium sized enterprises (SMEs); reduce delays and costs in cross-border remittances; foster efficiencies and transparency in government operations, which helps reduce corruption, and facilitate social and humanitarian transfers in a manner that preserves human dignity.

For the Middle East, North Africa, Afghanistan and Pakistan (MENAP) and Caucasus and Central Asia (CCA) regions, fintech has a particularly valuable role to play as these potential benefits are aligned with the regions' policy priorities. Both regions have countries with large unbanked populations, SMEs whose growth is constrained by limited access to finance, high youth unemployment, large remittance markets and informal transfers (Hawala), undiversified economies, vulnerabilities to terrorism, large income disparities, large displaced populations, and endemic corruption. Fintech innovations and underlying technologies can contribute to the solutions for many of these challenges.

The scale and pace of fintech in MENAP and CCA countries, however, lags other regions, and fintech is yet to foster an inclusive digital economy. Although there is significant diversity in the pace with which countries in both regions are adopting fintech, overall investment into fintech and the uptake of fintech and mobile financial services have been low compared to other regions. There also continues to be a strong preference for cash payments in the Middle East, despite the growth of e-commerce transactions. Consequently, the potential gap remains large in key areas such as financial inclusion, access to SMEs, diversification, reducing informal sector and the broader objective of inclusive growth.

This paper provides an overview of the fintech landscape in the MENAP and CCA regions and identifies policies to unlock fintech's potential. The report covers innovations in mobile and online banking, payments, lending and capital raising (P2P platforms, crowdfunding), money transfer platforms, digital currencies, digital wallets and adoption of emerging technologies (cloud computing and Distributed Ledger Technology (DLT) or blockchain). The analysis covers developments through the end of April 2018 and is based on both primary and secondary research, including interviews with selected central bank staff, legal and accounting firms based in the MENAP and CCA regions, presentations at conferences by management of fintech firms, speeches by central bank governors on issues affecting their countries and other analytical reports.

The study provides answers to five broad questions:

- What is the state of the fintech industry in the MENAP and CCA regions and what is driving its growth?

- What factors are constraining fintech from realizing its potential?
- Are there any financial stability risks emerging from existing fintech business models and how well do the regulatory frameworks balance the trade-off between promoting fintech and safeguarding financial stability?
- What is the value proposition for adopting fintech in the MENAP and CCA regions?
- What policies can help leverage fintech’s potential and contribute to the regions policy priorities of financial inclusion and inclusive growth?

The remainder of the report is structured as follows: Section II provides an overview of fintech, its definition, architecture, benefits and risks, and the required conditions to facilitate its sound development. Section III discusses the fintech landscape in the MENAP and the CCA, highlighting its scale, structure and growth drivers, regulatory and supervisory practices in the two regions, the risks and vulnerabilities posed by emerging business models and the factors hampering fintech growth potential. Section IV discusses the value proposition for promoting fintech in the MENAP and CCA regions. Section V summarizes the findings and discusses the policy options to unlock fintech’s transformative potential.

II. FINTECH: AN OVERVIEW

Fintech is the application of technology to deliver financial products and services, but the nomenclature has evolved to assume a variety of meanings. This study adopts the FSB (2017) definition of fintech as “technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services”.

The application of technologies in financial services is not new, but fintech represents a paradigm shift. For centuries, banks have undergone technology enabled revolutions, such as international transfers, electronic banking, the rise of credit cards and the emergence of Automatic Teller Machines (ATMs), which were designed to support bank operations. By contrast, fintech challenges and sometimes displaces traditional financial institutions and processes, elevates the role of data as a key commodity and drives the emergence of new business models. Fintech is also being driven by changing customer demands particularly from millennials that have grown in a digitally connected world and do not have the same loyalty to banks. While some consumers, particularly corporates, remain loyal to banks, changing consumer expectations are exerting pressure on banks to adopt internet enabled technologies to improve their services.

A visual depiction of the fintech architecture is presented in the schematic chart below (Figure 1). The technologies are not specific to the financial sector, but they play a significant role in fintech developments. They lower entry barriers and enable nonfinancial corporations² to offer financial services that traditionally were the preserve of regulated financial institutions while at the same time enabling incumbent banks to also develop new business models. The financial

² Big technology firms (Amazon, Apple, Alibaba), mobile network operators (MNOs), mobile transfer companies (MTOs) and large retail networks have entered the financial market place to offer payment and online lending solutions.

services targeted by fintech firms have, thus far, included payments, deposits, capital raising and lending, wealth management and insurance.

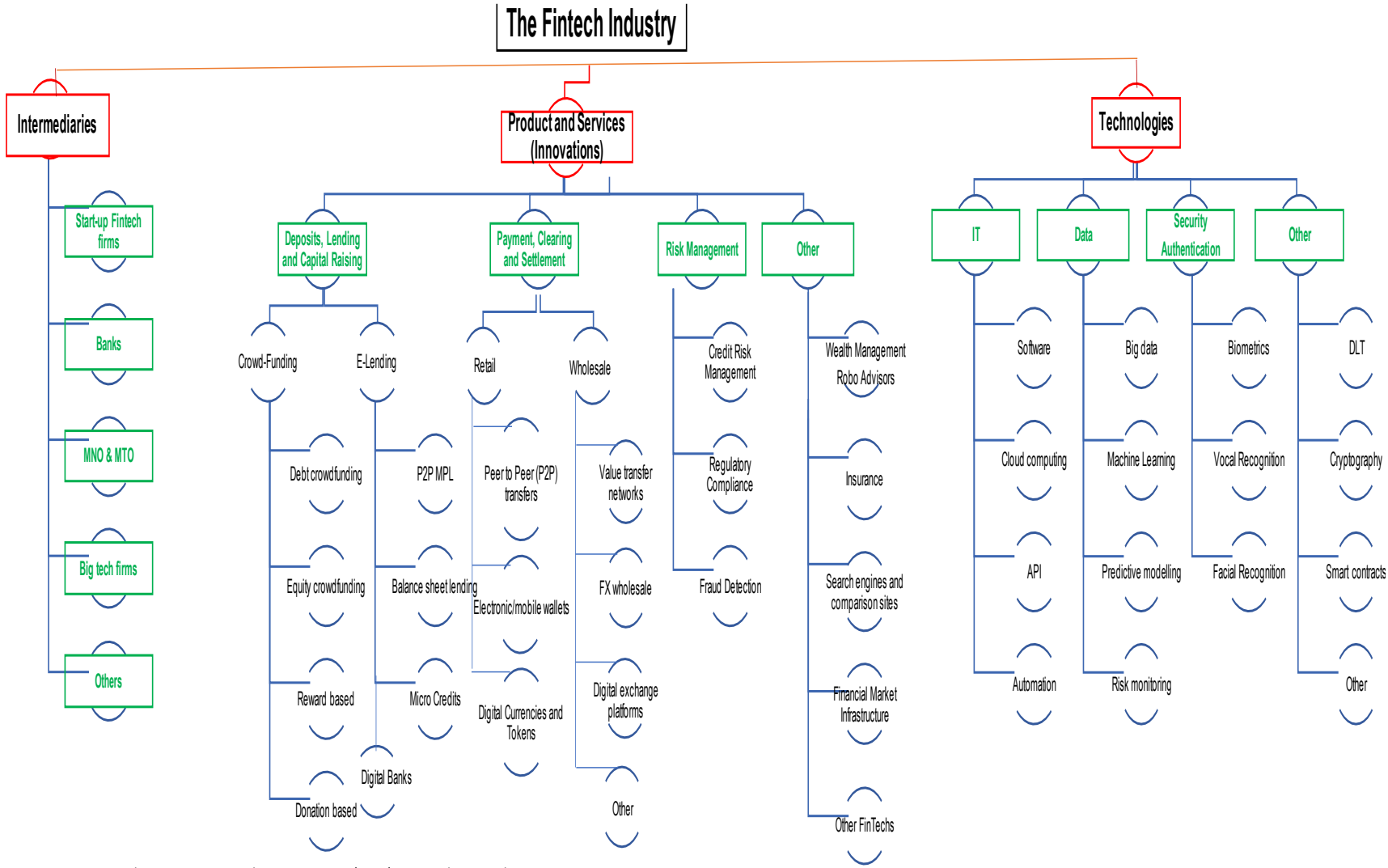
Technology-enabled business models change the sources and nature of financial stability risks. Some of the changes to the risk profile arise from new providers of financial services, such as Mobile Network Operators (MNOs), technology firms and the use of agents as the principal interface with customers. There are also risks from the digital technologies underpinning the new business models, new products and services, and the risk profile of financially excluded and underserved customers. These aspects of fintech impact cyber and other operational risks, money laundering, consumer protection risks, the regulatory perimeter and cross-border legal issues.

Cyber risks present a major challenge because of the potential systemic risks and interaction with other risks. Although cyber risks are not unique to fintech, increased connectivity and new entrants—that may not be subject to the same scrutiny as banks to ensure strong security systems—increase the entry points for cyber criminals and the potential for successful attacks. Cyber risks are also unpredictable, increasing in frequency and in sophistication. Successful cyberattacks can lead to monetary losses for financial institutions through denial of services or direct financial losses and can adversely impact financial institutions through data privacy breaches and related reputational risks as recent high profile cyberattacks demonstrated.³

But if the risks are well managed, fintech can confer far-reaching social, economic and financial stability benefits. Fintech facilitates lower-cost, faster, convenient, secure, and multi-channel accessibility to payments. It can also extend financial services to unbanked populations, lower SME funding gaps, reduce costs and delays in cross-border remittance markets, and improve efficiencies and transparency in government operations that help reduce corruption. The technologies underpinning fintech, such as Distributed Ledger Technologies (DLT) and Artificial Intelligence (AI), can help improve collateral management, fraud detection, credit risk management and regulatory compliance. Through these channels, fintech can reduce income disparities, and enhance financial inclusion as well as promote inclusive growth and financial stability.

³ Price Waterhouse and Coopers (PwC) Global Economic Crime Survey revealed that cybercrime has now jumped to the second most reported crime globally and that over half of organizations have been hit with cybercrime. Among many others, high profile breaches include the US \$81 million dollars heist from the Central Bank of Bangladesh, attacks on numerous Bitcoin marketplaces, such as Bitfinex, DAO and Ethereum, with Bitfinex, a Bitcoin exchange company, losing more than \$65 million in one day due to a security breach of multiple wallets, data breaches at Equifax which exposed personal information of customers, DDoS attacks that brought banks like HSBC to a standstill, and the hack at JP Morgan.

Figure 1. Architecture of the Fintech Industry

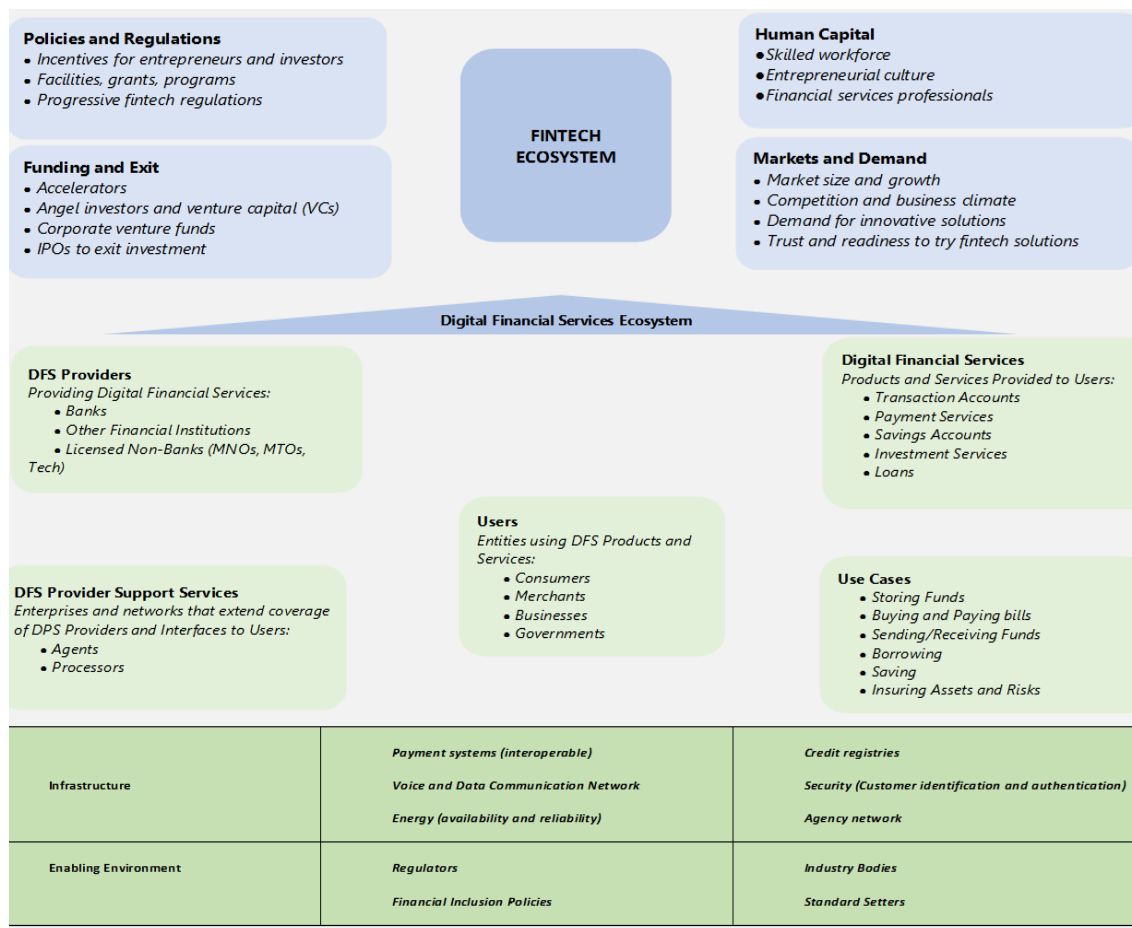


Source: Basel Committee on Banking Supervision (BCBS) 2018 and Inutu Lukonga

Cross-country experiences confirm the macroeconomic benefits of fintech and underscore the importance of balancing promotion of innovation with risk management. In advanced and emerging market countries (United Kingdom, United States and China), online lending platforms have contributed to increased lending to SMEs, albeit with different degrees of success. Several countries in Sub-Saharan Africa (SSA), such as Kenya, and in Asia, such as Philippines, have successfully deployed mobile payments to increase financial inclusion of unbanked populations, which has unlocked growth potential (Box 1).

The sound and sustainable development of fintech, however, requires enabling environments (Figure 2). In addition to sound macroeconomic environment, there is a need for a business-friendly environment, laws to provide legal certainty, prudential regulations that address fintech specific risks, financing across the spectrum of seed, venture and growth capital, talent in both technology and finance, IPO markets to facilitate investors who want to exit initial investments, and markets that create demand. These should be further supported by infrastructure comprising of affordable and widely accessible high broad band ICT and energy, interoperable payment systems, credit registries, digital authentication technologies, and a network of remote banking services, such as Point of Sale (POS), ATMs, Kiosks, Instant payment terminals.

Figure 2. Enabling Environment for Fintech

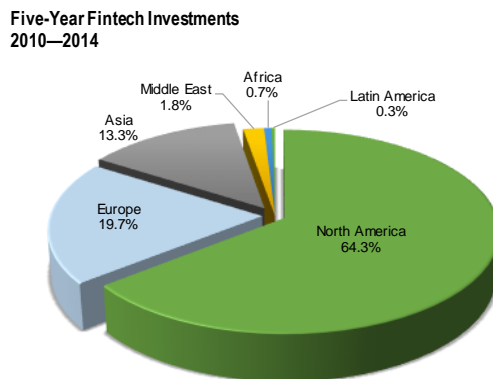


III. THE FINTECH LANDSCAPE IN THE MENAP AND CCA REGIONS

The MENAP and CCA regions was slow to adopt fintech, including mobile financial services (Figure 3). Fintech investments into the MENA region were estimated at less than 2 percent of the cumulative global investments between 2010-14 and this share has remained largely unchanged. Adoption of mobile payment services in MENAP also remains significantly below all other regions. Adoption of emerging technologies by banks varies considerably across and within countries, but many banks, particularly in many countries of North Africa, are yet to adopt even basic technologies, such as ATMs or credit cards. In the CCA, fintech and mobile financial services are in the nascent stage and many banks are also yet to implement basic technologies.

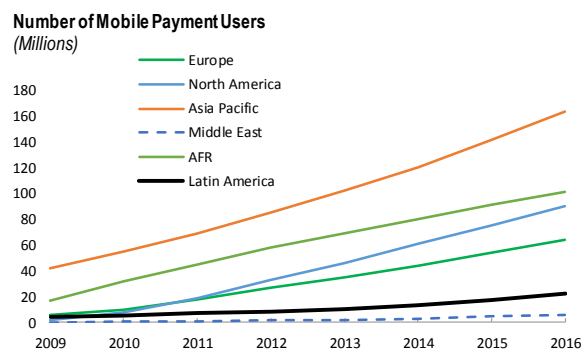
Figure 3. Scale of Fintech in the MENAP and CCA regions

The MENA was slow to invest in fintech...



Source: ITA Fintech Market Report, 2016.

The pace of mobile payment adoption has equally been slow...



Source: Statista

Since 2011, fintech has, however, been growing rapidly in importance and popularity in selected MENAP countries and is beginning to make inroads into the CCA. Between 2011-16, fintech startups in 12 MENA countries increased at a Compound Annual Growth Rate (CAGR) of 40 percent, going from 46 to 145 firms (Figure 4).⁴ Foreign fintech firms have also established operations, mostly in the GCC, alongside local fintech firms. Some local fintech firms based out of Lebanon and UAE have also grown into regional and international players (WAMDA 2016).⁵ Mobile financial services targeting unbanked populations, that first emerged in Afghanistan in 2008, have expanded to 11 countries by the end of 2017 (GSMA 2017).⁶ Banks are also making large direct investments in fintech with some countries (Bahrain, UAE, Pakistan) launching full digital banks. In the CCA, 63 fintech startups were established in Kazakhstan between 2013 and

⁴ In 2016, WAMDA undertook a survey of 12 countries, comprised of Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Tunisia, and UAE. Iran was not among the countries surveyed but a review of developments there shows rapid growth in fintech startups.

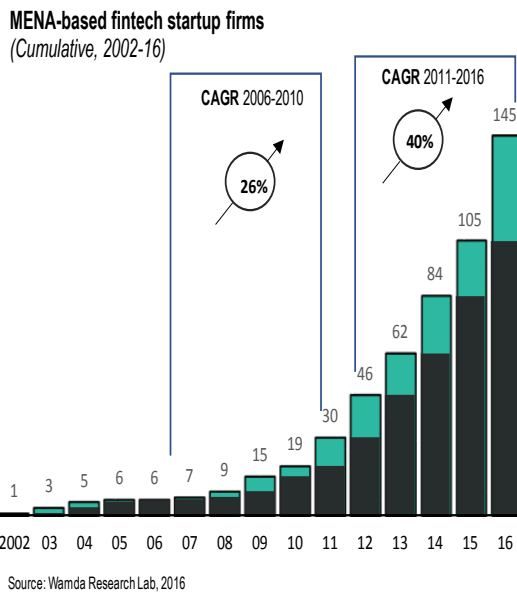
⁵ Foreign startups from the US, Europe, Australia and else-where have established presence in the MENA.

⁶ The countries include Afghanistan, Egypt, Iran, Iraq, Jordan, Mauritania, Morocco, Pakistan, Qatar, Somalia and Tunisia.

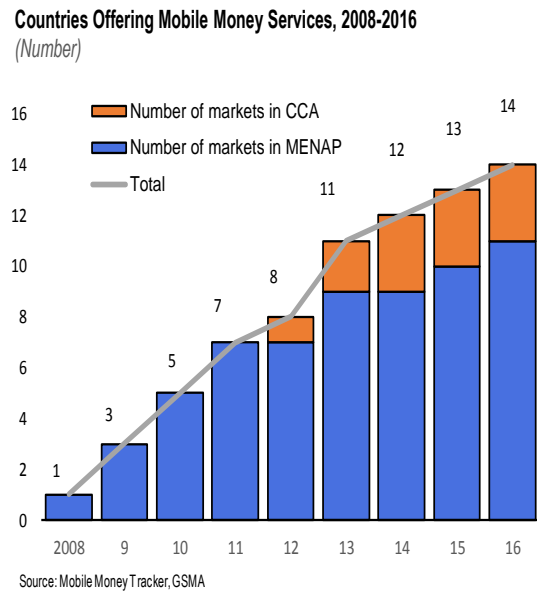
2016 (RCFA rating 2017), MNOs in selected countries (Armenia, Georgia and Kyrgyzstan) are offering financial services to unbanked populations (GSMA 2017, MMU tracker), and banks are increasingly adopting digital technologies.

Figure 4. Fintech Startups and Investments

Fintech startups in MENA more than doubled since 2012.



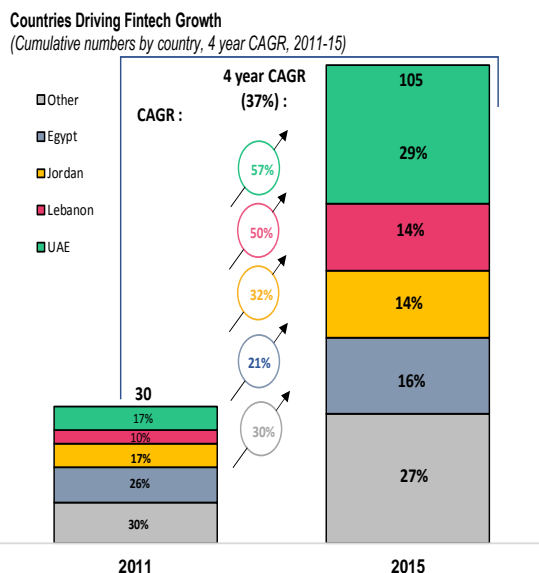
Countries offering mobile money services have also increased



Fintech activities are still concentrated in selected countries, but new growth centers are emerging. In the MENAP region, four countries (UAE, Lebanon, Jordan and Egypt) hosted 73 percent of the 145 fintech startups, with the UAE alone accounting for more than 30 percent (Figure 5). Nevertheless, after 2015, other countries (Bahrain, Iran and Saudi Arabia) have witnessed an acceleration in investments in the fintech sector. In the CCA, fintech activities remain concentrated in Kazakhstan, but there are some green shoots in other countries (Armenia, Georgia and Azerbaijan).

Figure 5. Geographical Distribution of Fintech Startups and Mobile Money Services

Fintech activities are geographically concentrated...



Mobile money services have slowly been expanding across the region

Geographic expansion of mobile money services
(2008-2016)

Year	MENAP Countries	CCA	Number of Countries (Cumulative)
2008	Afghanistan		1
2009	Pakistan		3
	Somalia		
2010	Tunisia		5
	Morocco		
2011	Qatar		7
	Iran		
2012		Armenia	8
2013	Mauritania		11
	Egypt	Georgia	
2014		Kyrgyzstan	12
2015	Iraq		13
2016	Jordan		14

Source: GSMA, MMU Tracker 2017.

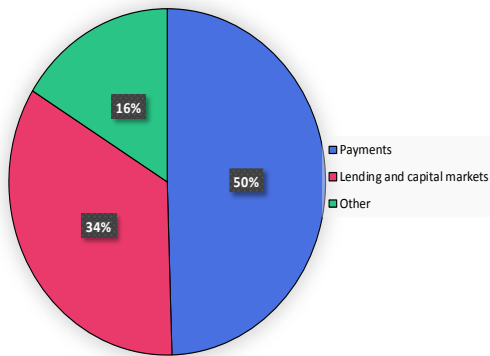
The payment segment has dominated initial fintech innovations, but the impact on financial inclusion remains limited. In MENAP, 50 percent of startups offered payment solutions, mostly retail⁷ (Wamda 2016, GSMA 2017), global technology companies (Apple Pay, Amazon) have established presence in selected countries (Saudi Arabia and UAE), Visa, a global leader in digital payments has been collaborating with local companies in the UAE to develop payment products, Alibaba Alipay, one of the largest digital wallet platforms in China, has entered the UAE and Bahrain has created a national e-wallet. However, in the Gulf Cooperation Countries (GCC), while banks are rapidly offering digital payments and mobile penetration is one of the highest in the world, mobile payments products for the unbanked populations are still limited (Ngatia 2017). In other countries, mobile money products for unbanked populations are developing fast, but from a low base. In the CCA, 40 percent of startups in Kazakhstan offer payment services; global payment companies (Mastercard) are developing cashless payments in Azerbaijan; and three countries (Armenia, Georgia and Kyrgyzstan) have developed mobile money products for unbanked populations, but volumes are low.

⁷ Payment solutions include bill payments, e-wallets and P2P transfers

Figure 6. Fintech Segments

The payment segment has attracted most of the investments in MENA...

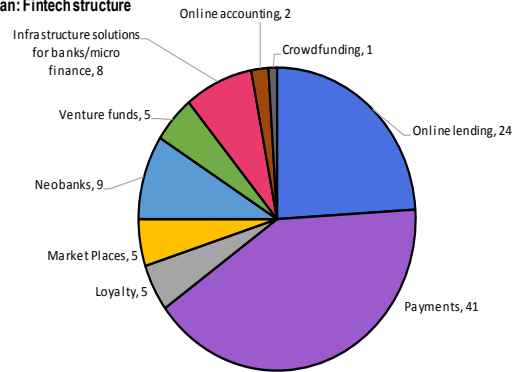
Sectoral Distribution of Fintech Startups in MENA



Source: WAMDA 2016
 Note: Reflects distribution of fintech innovations in the 12 MENA countries surveyed, including: Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Tunisia and UAE

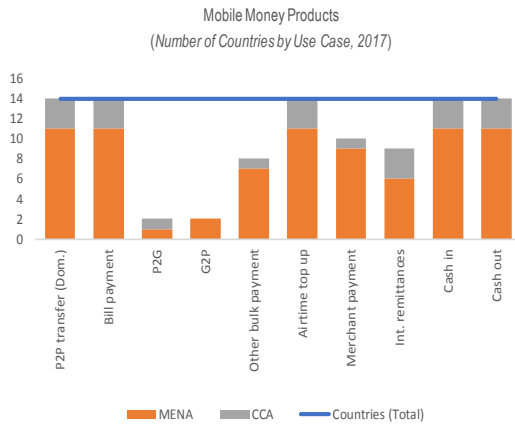
...and in the CCA too.

Kazakhstan: Fintech structure



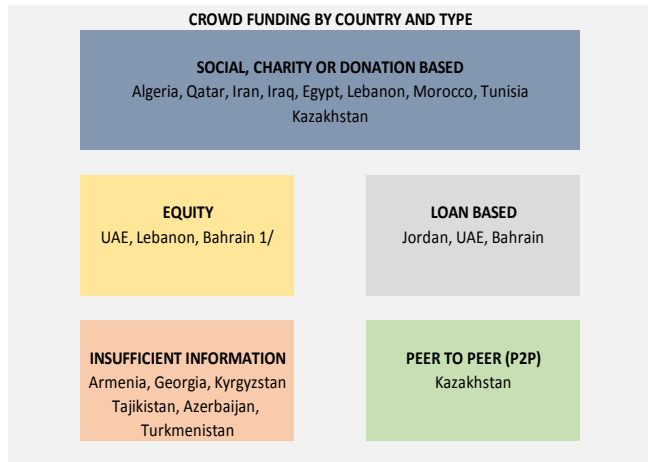
Source: RCFA Rating, 2017

Mobile products for international remittances, merchant and government payments are in early development stage



Source: GSMA (2017) Mobile Money Tracker.

Crowdfunding platforms exist in many countries, but most are social, charity or donation based



Source: Various. Staff Compilation

1/ Bahrain also has Sharia'h compliant equity based crowdfunding

Market place lending (crowdfunding) is the second-largest fintech segment, but the contribution to SME funding is still minimal. In MENAP, 30 percent of the startups offered lending solutions. Crowdfunding platforms have emerged across the region, but most are donation or rewards-based targeting social projects. The UAE, Jordan, and Lebanon are among the few countries with crowdfunding platforms that target SMEs (Figure 6), but credit intermediation through these platforms, while increasing, is still miniscule. In the CCA, 25 percent

of fintech startups in Kazakhstan provide online lending, mostly microcredits, and the failure rate of crowdfunding local platforms has been high, in part reflecting a lack of awareness and small market. Some local startups succeeded in raising funds through foreign crowdfunding platforms.

Cryptocurrencies are not recognized as legal tender, but trading and mining of cryptocurrencies is widespread, despite the regulatory headwinds. In MENAP, exchanges for cryptocurrencies have emerged in several countries (Bahrain, Egypt, Iran, UAE) as the meteoric rise in the value of cryptocurrencies and decentralized features lured investors.⁸ In the UAE, a Dubai-based firm (One gram) issued gold backed cryptocurrencies in 2018 to comply with Islamic principles, some fintech startups issued Initial Coin Offerings (ICOs), and some property managers began to accept cryptocurrencies for real estate purchases. In the CCA, banks in some countries (Georgia, Kazakhstan) installed ATMs for cryptocurrencies, some start-ups issued ICOs in Bitcoin and mining of cryptocurrencies is picking up in several countries (Armenia, Azerbaijan and Georgia).⁹

There is also growing interest in issuing national digital currencies encrypted on blockchain. In MENAP, Tunisia issued a national digital currency (the E-dinar) in 2015 and subsequently put the E-dinar on blockchain. The UAE (Dubai), in 2017, launched a blockchain-based encrypted digital currency called emCash and has been working with Saudi Arabia's central bank to issue a digital currency that would be accepted in cross-border transactions between the two countries. Efforts to develop a national cryptocurrency on blockchain are also advanced in Iran where cryptocurrencies are in high demand to counter the underdevelopment of the digital financial instruments caused by sanctions. Lebanon has also indicated interest in issuing national digital currencies. In the CCA, Kazakhstan has indicated plans to issue a national cryptocurrency.

New technologies are increasingly being embraced at national and bank levels, but the pace is uneven across countries, and some constraints to adoption persist. Blockchain has attracted the most attention, but adoption of AI and cloud computing is also on the rise. In MENAP, the UAE government has been at the forefront in developing strategies for the adoption of new technologies and some of the large banks have begun to deploy the technologies.¹⁰

⁸ The MENA was estimated to account for about 4 percent of global crypto currency exchanges in 2017 while Gulf investors were estimated to account for 1.5 percent of total value of cryptocurrencies (Cambridge 2017 and Arabian Business 2018). BitOasis, a legal platform where you can encash cryptocurrencies, was established in 2014 and operates in UAE, Saudi Arabia and Kuwait. The Bitcoin exchange in Egypt launched in 2017,

⁹ BitFury, the world's leading bitcoin mining company which mines about 15 percent of all Bitcoins, has established the largest cryptocurrency mining farm in Georgia, with data centers built in Tbilisi and Gori. As of 2017, Georgia was third in the list of biggest mining pools after China and U.S, propelled by tax exemptions and low electricity prices.

¹⁰ Banks in UAE have been on the fast track to implement blockchain technology with some banks introducing real time cross-border payments on blockchain and deploying blockchain to reduce fraud related to checks. Some banks in Qatar also announced the successful money transfer pilot by using a blockchain.

Other countries (Saudi Arabia, Tunisia, Jordan) are also making significant advances.¹¹ However, system-wide adoption of new technologies is not yet a reality, and banks in many countries are yet to adopt even basic technologies such as ATMs, debit and credit cards. Wider adoption of financial technologies is reported to be constrained by talent gaps, regulations, data security concerns, cost, and low infrastructure bandwidth (Al Tamimi and company 2017). In the CCA, block chain is also being deployed for land title registries (Georgia), and tax collection (Kazakhstan). There are ongoing experiments to use blockchain in remittance transfer (Tajikistan), but many banks are yet to adopt basic technologies.

Outsourcing to fintech firms is trending up as banks strive to meet customer expectations for digital financial services. In MENAP, banks in some countries are increasingly partnering with and/or outsourcing to third party service providers and fintech firms for solutions in a broad range of areas, including cloud solutions, digital transformation, artificial intelligence, blockchain, core banking system integration, smart payments, business intelligence tools, and cyber security. In addition, as many incumbent banks do not have the digital transformation acumen in-house, outsourcing is becoming integral to bank business strategies across the financial systems.

A. Growth Drivers and Prospects

The growth of fintech in the MENAP and CCA and the comparatively stronger performance of the UAE reflect the interaction of several mutually reinforcing factors. These include high consumer demand for digital products, increased investments in ICT, government support, and other idiosyncratic factors. For the UAE, the rapid growth of e-commerce and the increase in venture and private capital have provided additional stimulus. Going forward, favorable demographics, growing e-commerce and the increasing alignment of fintech with the policy priorities of diversification and financial inclusion increase prospects for greater adoption of fintech in the two regions.

High consumer demand for digital products and increased investments and competition in the ICT sector have facilitated broad based growth of mobile payments and fintech. In the MENAP region, the GCC are leading in internet and mobile phone subscriptions, reflecting the significant investments in fiber optics and digital cellular technologies and high smart phone penetrations that facilitated greater adoption of internet and mobile financial services. Within the GCC, the UAE, Bahrain, and Qatar have made the most advances, but Saudi Arabia has also accelerated investments in recent years while Kuwait has lagged somewhat after an early lead. The rest of the region exhibits great diversity with Jordan, Morocco, Tunisia, Egypt and Iran making greater strides while Pakistan, Algeria, Djibouti, Afghanistan, Somalia and Yemen lag the region. The CCA have also increased investments with Kazakhstan making the most advances followed by Azerbaijan, Armenia and Georgia.

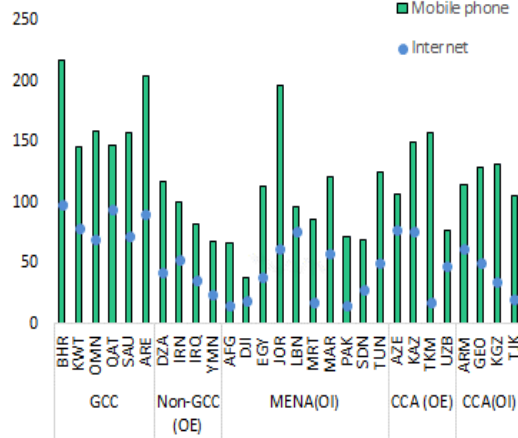
¹¹ In particular, SAMA signed a blockchain deal with Ripple in February 2018, Tunisia Economic City (TEC) a smart city project that is jointly owned with Saudi Arabia, is to apply the Locus Chain blockchain as its settlement currency and service platform.

Figure 7. Internet and Mobile Phone Penetration

High mobile and internet penetration and...

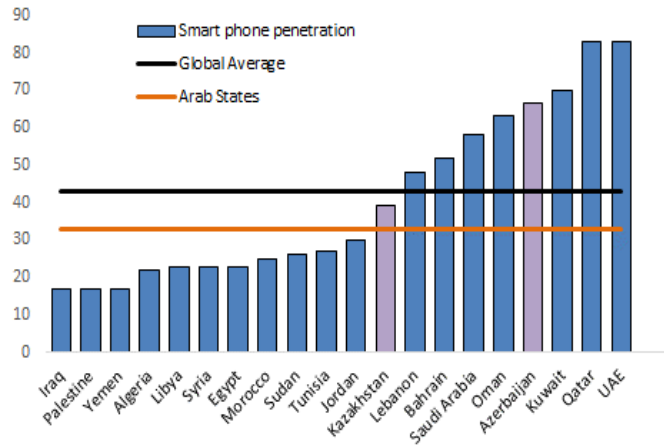
...high smartphone penetration have supported fintech growth

Mobile and Internet
(Percent of population, end 2017)



Source: ICTU, World Bank and GSMA.

Smart Phone Penetration
(Percent of population, June 2015)



Government support contributed to cross-country differences in the pace with which fintech is developing. The countries (the GCC, Egypt, Jordan, Lebanon, Kazakhstan) that established accelerators, incubators, and funding programs registered the most growth in fintech. Some of these countries (Lebanon) also offered fiscal incentives or created trade-free zones (UAE, Kazakhstan, Saudi Arabia). In addition, several countries (Bahrain, Egypt, Jordan, Kazakhstan, Oman, Qatar, Saudi Arabia, and UAE) accorded innovation a priority status in their strategic development agendas. Another group of countries have created demand for digital financial services by requiring e-payments for some governmental services (Egypt, Jordan, Oman, and Pakistan) or using mobile payments to pay salaries and social transfers (Afghanistan, Pakistan).

Availability of private capital funding for fintech has been a distinguishing factor in the comparatively stronger performance of fintech in the UAE. The bulk of private equity (PE) and venture capital (VC) flows into the MENA region has gone to the UAE. In 2017, UAE accounted for as much as 70 percent of total PE and VC flows (Figure 8). This, in large part, reflects Dubai’s status as a regional hub for expansion into other countries in the MENA and South Asia and government entities’ efforts to assist early stage ventures, including by providing a friendly regulatory environment for private capital.¹² Several other countries (Saudi Arabia,

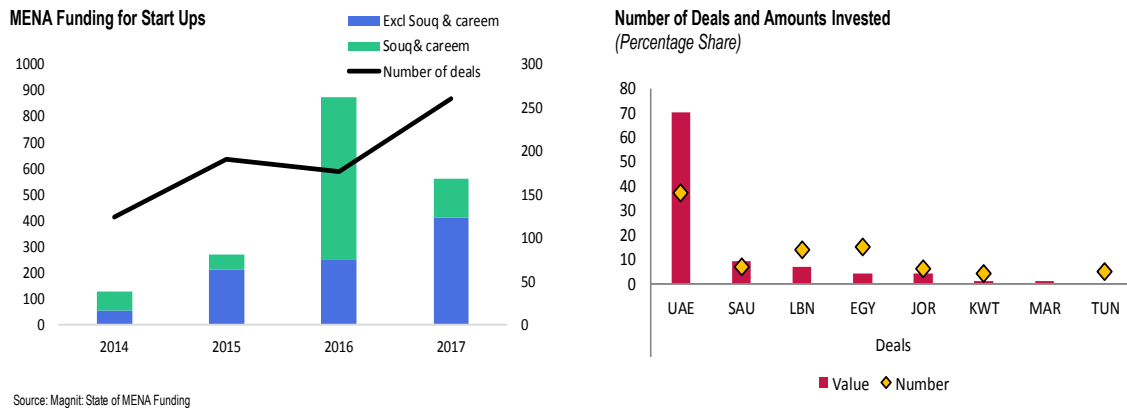
¹² Two free zones (Dubai Silicon Oasis in the Emirate of Dubai and twofour54 in the Emirate of Abu Dhabi) provide seed funding, training, and strategic advice for entrepreneurs in the Technology, Media and Telecommunication (TMT) sector. The Government of Dubai has also launched the "Dubai Future Accelerators" program, aiming to encourage young entrepreneurs to address the challenges facing the current age. Since 2015, the UAE has introduced new business friendly mutual funds regulations to stimulate the UAE funds industry and provide the foundation for a more developed regional funds regime in the Gulf Cooperation Council (GCC).

Egypt,¹³ Jordan, Oman, Qatar and Lebanon) have also registered increases, albeit of comparatively smaller magnitudes, in venture capital as government investment arms, central banks (Lebanon) and public institutions established VC and other funds to support startups.

Figure 8. State of Funding for Startups

Funding for startups in MENA has been increasing....

...led by the UAE.



Idiosyncratic and other country specific factors have also played a role in some countries.

In the MENAP, some countries (Somalia, Afghanistan) face weakened trust in incumbent banks, insecurity and related business uncertainty which has limited development of the traditional banking infrastructure and presented great opportunities for mobile financial services. On the other hand, Egypt’s giant consumer base has made it an attractive market for fintech while the high-net-worth but relatively small markets in the Gulf have encouraged a regional approach to fintech development. In the CCA, the banking crisis in Tajikistan is also leading to increased interest in mobile money and payments. Cold temperatures and low electricity costs have encouraged mining of cryptocurrencies in Georgia.

Prospects for fintech to grow rapidly are high for the MENAP and CCA regions, given the high latent demand.

MENAP countries have a high and growing share of tech-savvy millennials; growing e-commerce; large unbanked population; and underserved SMEs, migrant workers, and refugees.¹⁴ Policy makers, particularly in MENAP, have demonstrated a commitment to leveraging fintech as a tool for financial inclusion and economic diversification, and there is a continuing drive to promote cashless economies by mandating all government payments to be made electronically, including salaries, taxes, and fees. The CCA also has a large population of

¹³ The IFC has also been supporting venture capital (VC) funds, including in Egypt and UAE through WAMDA.

¹⁴ More than 60 percent of the population in the MENA region is younger than 25, E-commerce is growing rapidly in many countries (GCC, Pakistan, Kazakhstan), governments across the region are mandating electronic payments, including for fees, taxes and salaries, demand for remittance services are high given that foreign nationals account for about half the population in the GCC, with Qatar and UAE averaging close to 90 percent, and there are millions of displaced populations without access to bank accounts.

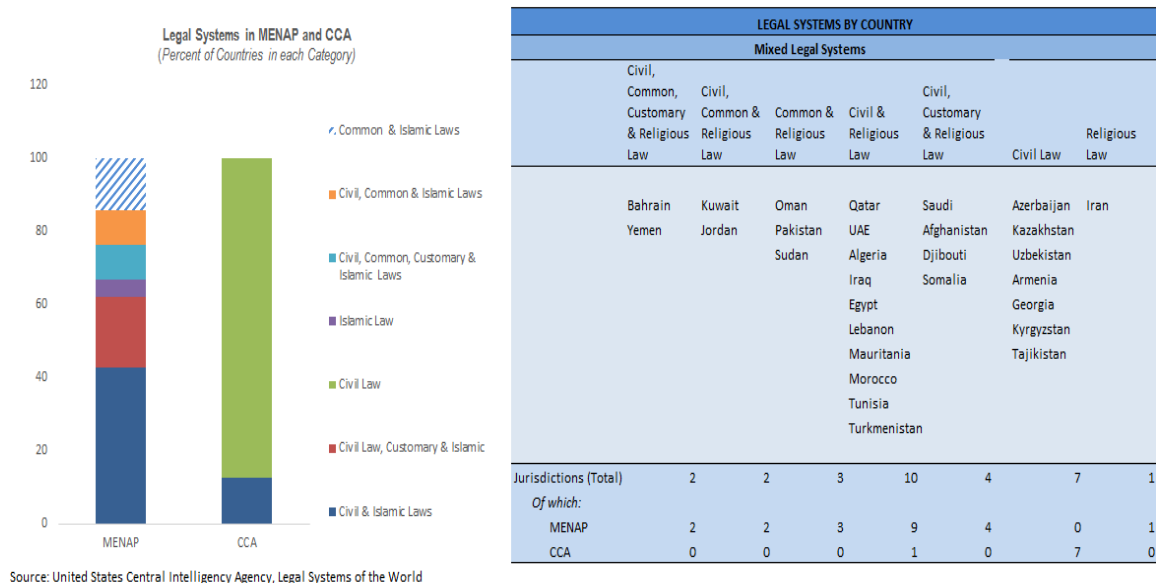
millennials and inward and outward remittance corridors, and though e-commerce is still underdeveloped,¹⁵ global e-commerce giants (Amazon) have begun to make their forays into selected countries (Uzbekistan).

B. The Legal Framework, Regulation, and Supervision of Fintech

Legal systems in MENAP and CCA are mostly founded upon civil law principles (Figure 9), thus legal certainty is a prerequisite for the development of fintech. In MENAP, most jurisdictions have mixed legal systems that are based on a varying combination of civil, religious, and customary law and only a few countries (Oman, Pakistan and Sudan) have legal systems founded on common law principles. The UAE in 2004 established the Dubai International Financial Centre (the DIFC) which has its own separate laws founded on English common law. In the CCA, all jurisdictions are based on civil law. Kazakhstan in 2015, however, established the Astana International Financial Centre (AIFC) with a separate legal framework based on English common law. Under civil law what is not stated in the law is generally not allowed, thus legal certainty and clarity is essential for the development of fintech.

Figure 9. Legal Systems in the MENAP and CCA

Most jurisdictions in MENAP have mixed legal systems based on civil law and all jurisdictions in the CCA are based on civil law



As in other regions, financial sector laws in the MENAP and CCA mostly predated fintech, thus legal issues unique to fintech have created gaps in the existing legal frameworks. However, given the backdrop of civil law systems, these regulatory gaps are more binding

¹⁵ Banks in some countries (Tajikistan) are still not technically ready to establish electronic payment system in local online shops.

because in civil law systems what is not in the law is prohibited.¹⁶ Many legacy laws include provisions for electronic money since card payments have been in place for several years. However, the provision of financial services by nonbanks (technology companies and MNOs) is a recent phenomenon, and legacy laws do not stipulate permissible organization, operation, functioning, and authorization of companies that offer alternative means of access to finance and investment, the issuance and management of electronic payment funds and the exchange of virtual assets or cryptocurrency. Similarly, many fintech concepts and instruments are not specified in the legacy laws.¹⁷ Laws, therefore, need to be updated to provide legal certainty to facilitate new entrants wanting to provide technology enabled financial services.

Reforms to close the legislative gaps caused by the emergence of fintech have commenced, but the pace is uneven across countries. Selected countries (UAE, Bahrain and Kazakhstan), that are aiming to be regional hubs, have proactively been amending their legal frameworks to address legal issues raised by fintech. Saudi Arabia is also considering changes and new licenses for fintech products and services are being developed. Several countries in MENAP (Egypt, Iraq, Jordan, Tunisia, Morocco, Pakistan) and in the CCA (Georgia, Kyrgyzstan) have introduced new laws on payments and payment systems to address emerging innovative payment instruments and the provision of payment services and remittances. Some countries (Mauritania, Tajikistan) are collaborating with the World Bank to modernize their payment systems laws. Central bank of Morocco, with technical assistance of the World Bank is working on the specific law on financial market infrastructure and means of payment oversight.

The Licensing Regime

The regulatory sandbox model, which provides firm-specific licenses for fintech, is being adopted slowly.¹⁸ In MENAP, there are currently four established sandboxes and two are in the process of development. Two of the established sandboxes are in the UAE DIFC, and the Abu Dhabi Global Market (ADGM), one is in Bahrain (established by the Central Bank) and another is in Saudi Arabia (established by the Capital Markets Authority in 2018).¹⁹ The Central Bank of Jordan and Saudi Monetary Authority (SAMA), in 2018, announced plans to establish regulatory sandboxes. In the CCA, the Astana Financial Services Authority (AFSA) in Kazakhstan introduced a regulatory sandbox in 2017.

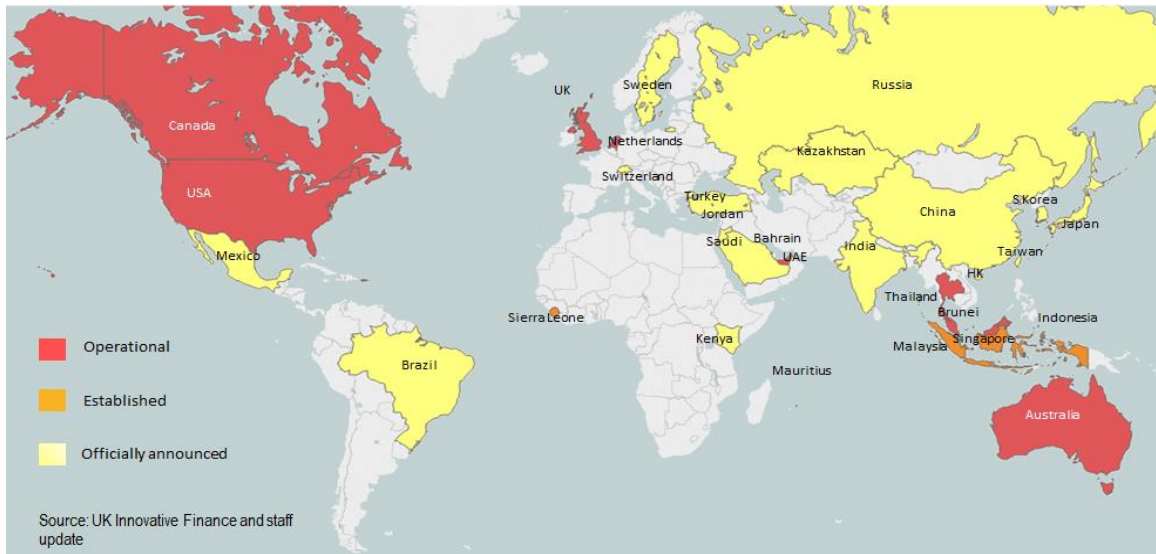
¹⁶ This contrasts with common law systems where everything is permitted that is not expressly prohibited by law, thereby providing more leeway for innovation.

¹⁷ For instance, legacy laws do not define many of the fintech concepts such as big data, crowdfunding, electronic wallets, prepaid cards or store of value facilities, virtual currencies, exchanges for crypto assets, regulatory sandboxes or Application Programming Interface (API).

¹⁸ Regulatory sandboxes are tailored frameworks that allow firms deploying innovative technology in the financial services sector ("FinTech participants") to develop, test and launch new financial products for a specified period without being subjected to the full suite of authorization regulation and rules from the outset.

¹⁹ The Saudi Arabia sandbox established by the Capital Markets Authority mainly covered securities activities.

Figure 10. Countries with Regulatory Sandboxes



Outside the free zone enclaves, there is a general lack of clarity and certainty on the licensing requirements for fintech. In the payment segment, selected countries (Afghanistan, Bahrain, Iraq, Jordan, Morocco, Tunisia, UAE) have created a new license category, which stipulates authorization requirements for nonbank payment service providers (PSP). Less progress has been made with respect to lending innovations, as only three countries (Bahrain, Lebanon, and UAE) have issued regulations governing the licensing and operations of crowdfunding platforms. Similarly, while many countries have warned about risks of crypto currencies, few countries (UAE) have enacted regulations to govern trading in virtual currencies or licensing requirements for digital exchanges. In the absence of adequate regulations governing fintech innovations, early fintech startups operating in MENAP and CCA are licensed in off-shore jurisdictions where there is either a specific enabling regime or where local requirements may be less onerous.²⁰

Prudential Regulations

The payments sector has registered the most progress in regulatory reforms, but gaps in the regulations and policy tensions are slowing the process of financial inclusion. In MENAP, some jurisdictions (Bahrain, Tunisia, Morocco, Iraq, Afghanistan, and UAE) have adopted operator-led models that allow nonbanks to issue e-money while others (Egypt, Pakistan, Yemen)

²⁰ For instance, CASHU, in 2016, became regulated under the stored value facilities licensing regime of the Monetary Authority of Singapore (MAS) and provides stored value cards across the Middle East for those without a credit card and enables them to make online transactions. Eureka registered in the Cayman Islands. Most of the P2P platforms operating in Kazakhstan are registered in Russia.

adopted bank-led models, which require nonbanks to operate through banks.²¹ In most other countries, legacy laws and regulations apply which creates some legal uncertainty about the permissibility of certain fintech innovations.²² In the CCA, bank-led models are the norm, and very few countries (Georgia and Kazakhstan) adopted operator-led models. While new laws have been enacted that address innovative payments products, less progress has been made in developing the regulations and rules regarding registration procedures, requirements, and standards for non-bank providers of mobile financial services. The adoption of bank-led models is designed to safeguard the stability of the payment system, but it inadvertently limits competition and scope to reach unbanked populations.

Crypto currencies and exchanges largely operate in a legal grey area, but there is a growing trend to ban them. In most countries, crypto currencies are unregulated either in terms of there being no legal framework in place, or the use of cryptocurrencies has been deregulated with no or very few legal restrictions. There also continues to be regulatory ambiguity in the few countries (Bahrain, Jordan and the UAE) that issued guidance.²³ Beginning in 2017, as cryptocurrencies came under increasing global regulatory scrutiny amid extreme price volatility and high profile incidents of cyber thefts, some countries (Qatar) prohibited financial institutions from trading in cryptocurrencies, some (Morocco) issued warnings about the risks linked to crypto currencies, another group (Egypt, Kuwait) issued “Fatwas”, and others (Pakistan, Saudi Arabia) banned trading in crypto currencies.

Crowdfunding regulations are not yet prevalent, and other laws necessary to support credit extension exhibit significant gaps. By the end of 2017, only three countries (Bahrain, Lebanon, UAE) had introduced crowdfunding regulations. Several crowdfunding platforms operating in the UAE and the GCC are domiciled in off-shore jurisdictions, but it is unclear whether the law offers the option to license abroad or there are gaps in regulations that can be exploited. In Morocco, the project law for crowdfunding is under progress and was published for public consultation in March 2018. Other laws— such as the protection of minority creditors and secured credit and insolvency— that are critical for equity crowdfunding and online lending to develop are also weak in many countries (Figure 11).

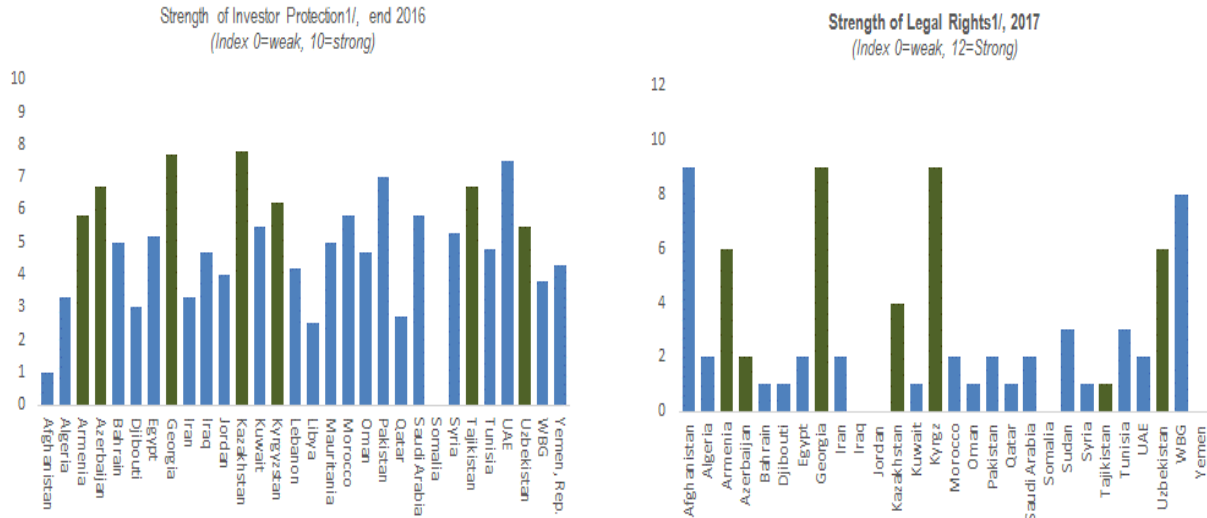
²¹ Operator-led models that allow nonbanks to issue e-money and increase potential of reaching populations not served by banks.

²² For instance, until recently, the lack of a legal framework for e-payment, among other reasons, had hampered the development of mobile payments in Algeria, whereas regulatory gaps in Somalia exposed customers to fraud and liquidity problems.

²³ The Securities and Commodities Authority stated that it doesn't recognize cryptocurrency fund raising, the Dubai Multi Commodities Centre (DMCC) issued licenses to allow firms trading in cryptocurrencies to operate from its free zone and the Central Bank of the UAE issued a ban that it later rescinded. In Bahrain, crypto currencies are allowed within the regulatory sandbox. Jordan issued a ban on trading crypto currencies but buying or selling crypto assets as well as organizing ICOs have remained technically legal.

Figure 11. Protection of Minority Creditors and Insolvency Regimes

Jurisdictions in the MENAP and CCA exhibit gaps in laws governing protection of minority creditors and secured credit and insolvency



Source: World Bank Doing Business 2018

^{1/} Measures the strength of minority shareholder protections against misuse of corporate assets by directors for their personal gain as well as shareholder rights, governance safeguards and corporate transparency requirements that reduce the risk of abuse

^{1/} Strength of legal rights index measures the degree to which collateral and bankruptcy laws protect the rights of borrowers and lenders and thus facilitate lending

Other Regulations Impacting Fintech Firms and the Adoption of Fintech by Financial Institutions

Cyber legislations are either at an early stage or under active development. In MENAP, several countries (Bahrain, Morocco, Oman, Saudi Arabia and UAE) have taken steps to enact cybercrime laws or introduced special systems. Some of the laws (Morocco, Oman and UAE) expressly aim at protecting electronic transactions and prosecuting cybercrimes (Aboul-Enein 2017). However, important gaps remain. The heatmap (Figure 12) shows the status of cyber security frameworks in mid-2017. In MENAP, out of the 21 countries, only one country (Oman) was reported to have a comprehensive cyber security framework that covered legal, technical, organization, capacity building and cooperation arrangements. In the CCA, only one country (Georgia) out of eight had a comprehensive cyber security framework, and progress in developing the legal framework has been uniformly slow.

Figure 12. Status of Cybercrime Legislations in the MENA and CCA, June 2017

Cybersecurity Scores (Index)	Cybersecurity Scores (Index)				
	Legal	Technical	Organisation	Capacity Building	Cooperation
BHR	Green	Red	Yellow	Red	Yellow
KWT	Red	Red	Red	Red	Red
OMN	Green	Green	Green	Green	Green
QAT	Green	Green	Green	Green	Green
SAU	Green	Green	Red	Green	Green
UAE	Green	Yellow	Yellow	Yellow	Yellow
DZA	Green	Red	Yellow	Yellow	Yellow
IRN	Yellow	Yellow	Yellow	Yellow	Yellow
IRQ	Red	Red	Red	Red	Red
AFG	Red	Red	Yellow	Red	Yellow
DJI	Red	Red	Red	Red	Yellow
EGY	Green	Green	Yellow	Green	Green
JOR	Red	Red	Yellow	Yellow	Red
LBN	Red	Red	Yellow	Red	Yellow
MAU	Red	Red	Yellow	Red	Red
MAR	Green	Green	Yellow	Yellow	Yellow
PAK	Yellow	Red	Red	Red	Green
SOM	Red	Red	Red	Red	Red
SDN	Yellow	Red	Red	Red	Red
TUN	Green	Yellow	Red	Yellow	Yellow
AZE	Red	Green	Red	Yellow	Green
KAZ	Yellow	Green	Red	Red	Red
TUK	Yellow	Red	Red	Red	Red
UZB	Yellow	Yellow	Yellow	Red	Red
ARM	Red	Red	Red	Red	Yellow
GEO	Green	Green	Green	Green	Green
KGZ	Red	Red	Red	Red	Red
TJK	Yellow	Red	Yellow	Yellow	Red

Green = In place Yellow = Deficient Red = Absent
 Source: International Telecommunication Union (ITU)

Consumer protection frameworks for financial services exist in many MENAP and CCA countries but most predate fintech, thus gaps and conflicts have emerged. With very few exceptions (such as Sudan), countries in both regions have consumer protection frameworks for financial services (World Bank 2017). However, mobile payments introduce new consumer protection risks, including lack of tangible proof of payment, dormant assets in electronic wallets, absence of viable dispute resolution mechanisms, the absence of digital certification in generic mobile phones that increases the risk of fraud and protection of consumer funds in bankruptcy.²⁴ Equity crowdfunding against the backdrop of weak minority shareholding protections also present investor protection risks. Some tensions have also emerged between the policy objectives of financial stability and financial inclusion.²⁵

Data protection laws that are integral to consumer protection also exist in many MENAP and CCA countries, but fintech presents new challenges. In MENAP, virtually all countries (excluding Pakistan) have data protection and privacy laws, but these mostly consist of piecemeal provisions that are diffused in various sectoral laws. In addition, while data are at the center of

²⁴ In mobile payments the treatment of dormant assets in the case of number termination, loss of phone and death is not adequately addressed. E-money issued by MNOs are also not treated as deposits and are, therefore, not covered by deposit insurance.

²⁵ For instance, to safeguard financial stability in mobile payments, some countries in MENAP (Pakistan, Egypt) and most CCA opted for bank-led models where nonbanks interface with customers is through banks. However, bank-led models inadvertently limit competition and scope to reach unbanked populations.

fintech, and governance and privacy assume greater importance, there is a lack of clarity on what qualifies as personal data, who is responsible and the penalties for data breaches (DLA Piper 2017; Aboul-Enein 2017). To address data privacy and security related to use of the cloud, in Saudi Arabia issued a cloud computing regulatory framework (CCRF),²⁶ Bahrain issued new regulations that address privacy issues and some countries (UAE) require that data be stored locally when using the cloud.²⁷ In Morocco, the critical infrastructure must host on the national territory, data which are sensitive in terms of confidentiality, integrity or availability. All CCA countries also have data protection frameworks that are diffused in various legal acts and which do not define sensitive data, while enforcement falls under multiple bodies. In Kazakhstan, processing of data in the cloud is permitted but storage is only allowed through local databases (ICLG 2017).

AML/CFT regulatory frameworks have been established in all countries but implementation of risk-based frameworks critical for financial inclusion has been uneven.

In MENAP, a few countries (Pakistan, Morocco) have passed regulations that contain provisions for simplified consumer due diligence (CDD) and tiered Know Your Customer (KYC) requirements. The UAE have issued regulations that have some elements of tiering but the risk based concept is not fully integrated or implemented. Several countries (Bahrain, Oman, Somalia, Egypt) have not eased KYC requirements for retail payments and, in some cases (such as Somalia), KYC rules in mobile payments have even been further tightened due to concerns about terrorist financing. In the CCA region, past assessment identified significant deficiencies and few countries have recently completed their AML/CFT assessments.

Regulations governing outsourcing to third party providers by financial institutions exist in many countries, but fintech has created new regulatory gaps alongside existing ones.

Outsourcing regulations of many countries in MENAP and CCA do not provide adequate clarity on access, audit rights, chain outsourcing or subcontracting, contingency plans, exit strategies, location of data, processing and security, including for cloud. In very few countries (Saudi Arabia, UAE) do the prudential regulators have authority to directly supervise third-party service providers or activities provided by third-party service providers to licensed financial institutions (FSB 2017). In some (Kazakhstan) the existing guidance does not address due diligence elements, aimed at ensuring an effective control environment and access for the regulator to assess the service provider. Financial Sector Assessment Programs (FSAPs) have also not given due attention to outsourcing regulations.

²⁶ The Cloud Computing Regulatory Framework (CCRF) entered into force in March 8, 2018.

²⁷ Data and cloud computing is central to fintech business models and small population sizes of many countries in the region make it imperative for fintech firms to adopt a regional focus to scale up to profitability. Thus, while the local content requirement addresses sovereignty concerns, "local content" requirements for data can presents some operational challenges for fintech firms with cross border operations.

Supervisory Frameworks

Supervision of fintech largely reflects the existing financial regulatory architecture, but some countries have begun to modify their institutional framework. At least four countries (Bahrain, Iran, Pakistan and UAE) have either modified their supervisory structures to take account of fintech or have proposed such changes. Bahrain²⁸ and Pakistan established special units to oversee fintech, oversight of fintech in the UAE is provided by multiple bodies (Central bank and DFSA) with overlapping mandates and Iran has proposed a separate regulatory body for monitoring and supporting innovative services. In others (Egypt, Jordan, Lebanon, Morocco, Saudi Arabia), the central banks have supervisory oversight as part of their oversight responsibilities on banks and payment systems.

Surveillance of fintech activities and cyber risk preparedness in banks is still patchy. Few countries, if any, provide information on authorized fintech firms and their performance as is done for banks. Some progress has been made in capturing payment transactions but no official data are available on credit intermediation through the online platform lenders. A few countries (Saudi Arabia) have begun stress tests for cyber risk preparedness, and others (Bahrain) now cover cyber risks in their Financial Stability Reports. Oversight of operational risks has received increasing attention since the introduction of Basel II, but little information was available on the management of key risks, such as IT audits and oversight of outsourcing to third parties, including in FSAPs.

Cross-sector and cross-border collaboration mechanisms to cover fintech firms have begun to develop in a few countries. The entry of nonbanks in the financial market place, such as technology firms and MNOs, requires collaboration between banks and the regulators of the nonbanks, but institutional mechanisms to facilitate that collaboration are yet to be developed. Efforts are already underway to strengthen cross-border cooperation and harmonization for fintech at the global level (IMF 2017), but implementation is still too early for many countries in MENAP and the CCA regions. Selected national regulators (UAE, Bahrain) have put in place cooperative arrangements to promote innovation and share information about innovative financial services.²⁹

C. Cyber Risks and Other Vulnerabilities

The current scale of fintech markets in the MENAP and CCA is still too small to disrupt banking systems, but cyberattacks, data privacy, and security breaches present important challenges. As fintech and mobile financial services scale up, outsourcing risks, consumer

²⁸ Bahrain established a Fintech and innovation unit in October 2017 that is responsible for the approval process to participate in the Regulatory Sandbox, supervision of licensed companies' activities and operations, including cloud computing, payment and settlement systems and monitoring technical and regulatory developments.

²⁹ The Bahrain Economic Development Board (EDB) and Abu Dhabi Global Market (ADGM) entered into a Fintech cooperation agreement. In addition, the EDB signed agreement with Singapore Fintech Consortium, ADGM and Dubai Financial Services Authority (DFSA) entered into an agreement with the Monetary Authority of Singapore to develop a fintech ecosystem.

protection risks, money laundering, regulation of nonbanks, and IT risks could assume greater importance. Some of the risks are mutually reinforcing and, therefore, may result in non-linear effects on financial systems.

Cyber Security Risks and Data Breaches

Cyberattacks constitute the biggest threat due to their increasing frequency, unpredictability, potential for systemic impact, and existing gaps in risk management.

Cyber risks are not unique to fintech but increased interconnectivity driven by financial technological developments increase access points and the potential for cyberattacks to have system-wide impact. Successful cyberattacks could also erode confidence in technology-driven business models, slow-down the uptake of digital financial products, and hamper the overall development of the fintech industry. Cyber risks are further heightened by the diverse, complex, and increasing threat landscape, significant deficiencies in cyber security risk management frameworks (Figure 12), and the increasing interconnections in financial systems.

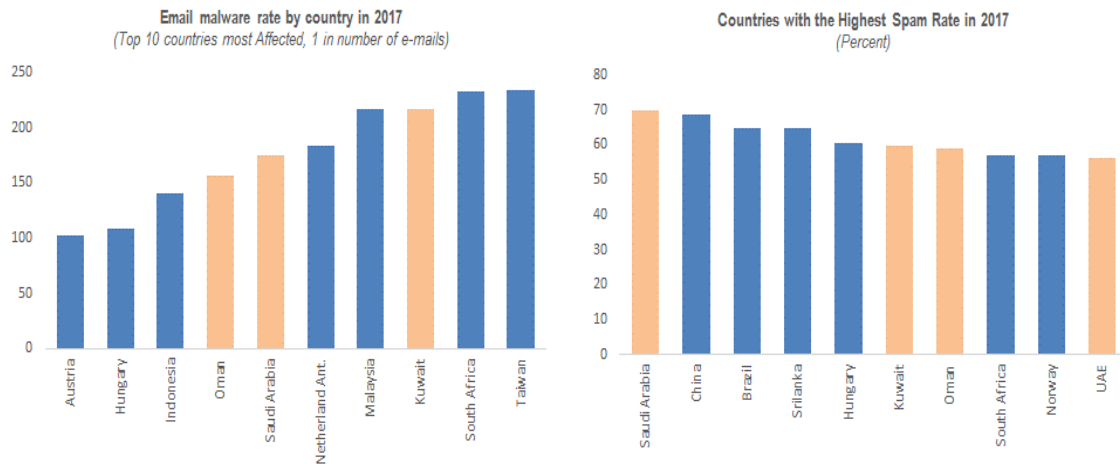
Though the MENAP and CCA have not had high-profile cyberattacks, there have been several incidences of successful attacks on individual financial institutions (Box 3). In MENAP, cyber criminals hacked into two card processing centers in India that handled payment processing for prepaid cards for banks in the UAE and Oman and withdrew U.S. 45 million dollars from ATMs in 27 countries. The UAE have also been a target of several cyberattacks that included ATM skimmer malware that resulted in both financial losses for customers and data privacy breaches. In Qatar, cybercriminals hacked into one of the largest banks' security system and exposed client information. Websites of central banks and securities exchanges in UAE, WBG and Saudi Arabia were also disrupted. In the CCA, several banks have been targeted by cyber criminals, using phishing scams (Kazakhstan), ATM skimmer malware (Armenia, Georgia and Kyrgyzstan), infiltration of bank computers (Armenia and Azerbaijan) that resulted in financial losses and data privacy breaches. Armenian and Azerbaijani cybercriminals also have a history of targeting each other's cyber space due to geopolitical tensions between the two countries.

The threat landscape for MENAP and the CCA countries shows that cyberattacks are increasing in volume, diversity, and complexity. Symantec cybersecurity threat intelligence reports (2018) indicate that in the MENA, the UAE was the second most targeted country for ransomware attacks, behind Saudi Arabia, and ranked 26th worldwide. Several GCC member states (Kuwait, Oman, Saudi Arabia and UAE) have also emerged among the top 10 countries that are targeted globally using email malware and spam (Figure 13). The threat landscape in MENAP is also made worse by the geopolitical tensions that open avenues for state sponsored and terrorist motivated cyberattacks. In the CCA, Kazakhstan is the most targeted, but other countries are also facing increased attacks.³⁰

³⁰ Kazakhstan has been a target to 85 percent of internet-based attacks compared with 8 percent in Uzbekistan, 4 percent in the Kyrgyz Republic, 2 percent in Turkmenistan, and 1 percent in Tajikistan (UNIPATH 2016).

Figure 13. Cyber Security Threats

The GCC are among the most targeted countries by cyber criminals



Source: Symantec, Internet SecurityThreat Report, Vol 23

The financial landscape for MENAP and CCA also exhibits vulnerabilities that increase potential for cyberattacks to be successful. Cyber security frameworks in both the MENAP and CCA remain deficient in a broad range of areas, including regulations, technical, organization, capacity building, and cooperation (Figure 12). In the MENAP, policy-makers in several countries (GCC) have increased attention to cyber risks, and investments in cyber technology are reported to be high and increasing, but the investments in employee training have not kept pace and governance structures are not well developed.³¹ The MENAP is also reported to be lagging the rest of the world in developing processes connected to cybersecurity, including identity management, threat assessments, vulnerability assessments, and security standards for external business partners (PwC 2016). In the CCA, deficiencies in the cybersecurity frameworks are also very widespread.

Increasing interconnections in financial systems will continue to elevate cyber risks. In both MENAP and CCA, countries are beginning to prioritize the development of highly skilled and service-oriented private sectors as part of the diversification effort. National economic transformation programs in Egypt, Kazakhstan, Qatar, Saudi Arabia, and UAE call for the expansion of smart cities, e-commerce and automation driven industries. Digital applications can also affect the burgeoning banking sectors in Bahrain, Qatar, and Jordan by automating payments, data processing, and customer interactions. Central to this development is the increasing application of digital technologies centered around networking, cloud computing, and data storage. Meanwhile, despite a sharp increase in the migration of sensitive data to the cloud,

³¹ Studies covering the Middle East (PwC 2016) show that employee mistakes and third-party service providers are the major threats to sensitive data.

most companies do not have a consistent encryption strategy in place, which is vital to protecting sensitive data against cyber criminals and guarding against human error (Thales 2018).

Other Risks

The risks of fintech startups disrupting incumbent banks are considered low, but selected income streams could be at risk. Corporate lending in the GCC remains relationship based, thus banks continue to enjoy a strong customer base. In other countries, the large unbanked populations provide space for mobile payment innovations to complement, rather than displace, banks. However, banks that are slow to embrace fintech risk losing market shares to those that succeed with their innovation strategy. Selected business lines for banks, such as money transfers, could face intense competition for fintech (S&P 2017).

Cryptocurrencies do not appear to pose financial stability risks yet, but they could should their use become more widespread without appropriate safeguards. Though the MENAP and CCA have been strengthening their AML/CFT frameworks, many countries are exposed to terrorist activities and proximity to conflict zones that increase the risk of cryptocurrencies being used for illicit activities like money laundering and terrorism financing. Risks may also stem from involvement of non-traditional players, which may not be strictly regulated for AML/CFT purposes and are not obligated to detect and report suspicious activity (Tanai 2014). Crypto assets have also been afflicted by fraud, security breaches, and operational failures and may raise issues about investor and consumer protection, money laundering, and tax evasion (IMF 2017b).

Fintech also presents new consumer protections risks alongside traditional ones. The entry of nonbanks in the financial market place do not in themselves pose risks, but if regulatory oversight is weak, then innovative products such as “prepaid store of value facilities” could put consumers funds at risk, if there is misuse of funds, PSPs become insolvent or agents do not have enough liquidity to meet “cash-out” demands.³² The growth of e-commerce also exposes consumers to cross-border disputes and data breaches depending on the way consumer’s personal information is collected, transferred, and stored. Additionally, due to the relative newness of many fintech companies, business resiliency and financial viability are also potential vulnerability.

Other operational risks, such as IT outages, could become important in countries with unreliable provision of electricity and internet service. The growing trend to shift to digital modes of delivering financial services requires reliable electricity and internet. Unreliable electricity supply remains a significant problem in some countries (Egypt, Lebanon, the West Bank and Gaza, and Yemen), and this can lead to service disruptions as financial institutions rely more on internet for service delivery (EBRD, EIB and World Bank 2016).

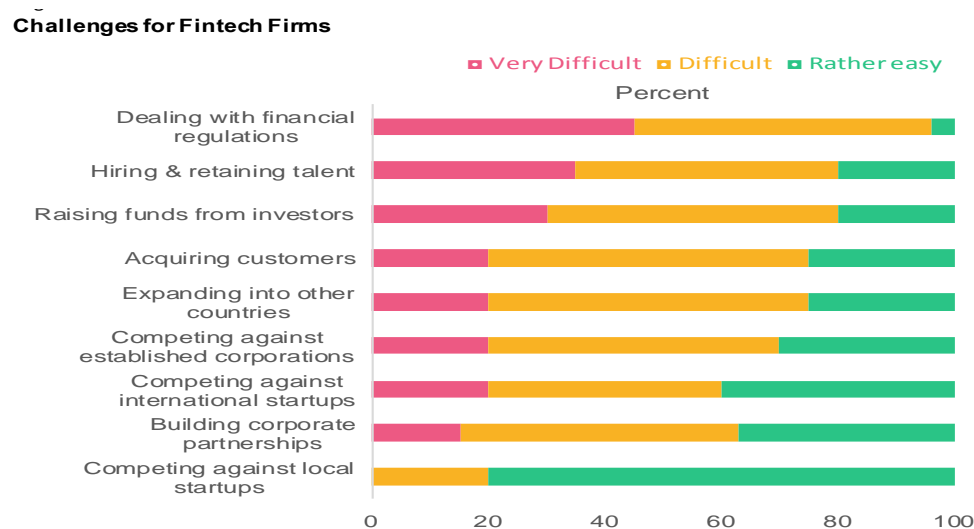
³² Funds held as stored value with a DFS provider are not generally considered to be a bank deposit and are usually not covered by any depositor protection scheme.

Regulatory and supervisory gaps could emerge that create opportunities for cross-sector and cross-border regulatory arbitrage. Non-bank payment service providers, such as telecommunication and technology companies, do not immediately fit neatly into the jurisdiction of any specific regulatory authority, or there may be ambiguity as to which authority is responsible for the non-banks. In MENAP, some non-banks have cross-border operations and some licensed their operations in countries that are outside the region, but collaboration arrangements between the home and host regulatory authorities have not yet been determined. In the CCA, Kazakhstan plans to be a regional hub, thus cross-border operations for fintech can be expected. Overall, the flood of fintech solutions and the speed of developments pose challenges for the regulatory formulation process, both in terms of pace and skills.

D. Factors Impeding Fintech Growth and its Impact on Inclusive Growth

Fintech in the MENAP and the CCA regions faces significant obstacles that hamper its growth potential and limited its impact on financial inclusion. Key constraints identified by fintech firms are the gaps in regulations, talent, and private capital coupled with demand factors, including lack of trust (Figure 14). A restrictive business environment, infrastructure gaps, low financial literacy levels, and socio-political factors also present major challenges. These factors are not all present to the same degree across countries but have contributed to the high failure rate of fintech start-ups in both regions and the stifling of fintech in the CCA.³³ They also act as inhibitors to faster growth of mobile financial services and the attainment of the broader objectives of financial inclusion and inclusive growth.

Figure 14. Key Challenges Facing Fintech Firms



Source: Wamda Research Lab, 2016

³³ In the MENA, the failure rate of fintech firms is currently estimated at 28 percent (Wamda 2016) and Kazakhstan is also reported to have had a high failure rate of crowdfunding platforms.

Regulatory constraints assume a variety of forms. These in the main include regulatory gaps, ill-suited regulations, complex institutional frameworks for regulation, lack of harmonization in laws, and other restrictions.

- Regulatory gaps constitute a major barrier for entry into the fintech industry given the backdrop of civil law environments. In civil law what is not expressly permitted is usually not allowed—unlike in common law countries where the absence of express laws prohibiting new developments may create space for innovations to develop. Lack of regulatory clarity around the use of the cloud, concerns with data residency, and security are also reportedly hampering uptake of cloud computing (Gartner 2017). Similarly, the absence of crowdfunding regulations and gaps in laws governing investor protection and insolvency hamper the development of market place lending or forced platform providers to license abroad.
- Legacy laws are ill-suited for technology-driven business models. Licensing requirements, such as large minimum capital for firms providing intermediation services, may be onerous for fintech business models such as platform lenders.
- The current scattered institutional landscape for licensing and regulating fintech also presents challenges for fintech firms. Rapid fintech developments require that all involved domestic agencies cooperate (central bank, financial regulator and supervisors, financial intelligence unit, securities supervisor, relevant ministries, telco supervisor, internal revenue authority), and this layering presents major challenges for firms.
- The lack of harmonization in cross-border laws presents challenges for the growth of fintech. Many countries in the MENAP and CCA have small populations, and this can make it difficult for firms to achieve scale and profitability without expanding abroad.
- Restrictions on the role of agents and nonbanks in financial service delivery and extensive customer ID requirements also slow efforts to extend financial services to unbanked populations.

The talent gap is another important headwind for fintech startups in the region. Despite relatively heavy spending in education by countries and while some countries (Egypt, Jordan, Lebanon) have developed substantial talent in technology skills, the labor market for many countries has not been adequately aligned with the needs of a digital economy in many countries. In MENAP, startups— especially those at the forefront of cloud computing, cybersecurity, machine learning, or artificial intelligence— report challenges in attracting and retaining the talent they need to succeed. In the GCC, individuals with technology and finance skills tend to be drawn toward large corporations, such as banks or the public sector, where salaries are higher. Underfunded startups, also are unable to offer globally competitive salaries and incentives to attract skills from outside (WAMDA 2016). Governments across the Gulf and Levant are already taking steps to promote and fund technical education with the hope of alleviating both youth unemployment and the digital talent shortage over the medium- to long-term. Some countries (UAE) have begun to reform entry visas for investors and professionals.

The underdevelopment of capital markets remains an important constraint for firms, including fintech. Though private equity and venture capital has registered noticeable growth, it is concentrated in a few countries and remains scarce for most countries (Figure 8). Fintech firms cite the lack of seed, venture and growth capital funding necessary to bring start-ups to sufficient scale and profitability.³⁴ Regional conflicts also discourage investment and put a damper on the region's budding venture capital activity and external capital. Capital markets in many countries are also not of sufficient depth to facilitate venture capitalists exiting their investments easily. In the CCA, the private equity and venture capital market is even more underdeveloped.

Gaps remain in ICT, payment, and credit information infrastructure, and there is also a digital divide in the regions, particularly in the MENAP region. Low-speed 2G networks³⁵ account for over 40 percent in MENAP and 58 percent in the CCA. 4G coverage is uniformly low, and this can hamper uptake of cloud computing with adverse consequences for fintech startups to scale up and SMEs as well (Figure 15).³⁶ Very few countries (Pakistan, Egypt and Jordan) also have interoperable mobile network systems or wallets, and this fragmentation in the market constrains financial inclusion (GSMA 2017). Banks' legacy infrastructures, on the other hand, hamper adoption of new payment systems and penetration of ATMs and POS terminals is low, which adversely affects mobile users' ability to "cash in" and "cash out".³⁷ There is also a digital divide in the penetration levels of ICT infrastructure, with conflict countries having low penetration levels as instability has made it difficult for MNOs to function. Coverage of credit registries remain low, which hampers development of market lending innovations.

³⁴ In the UAE, for instance, 83 percent of the 100 start-ups surveyed were funded fully or partially from the personal savings of their founders, 10 percent had received funding from Angel investors and 4 percent from venture capital and another 4 percent from crowdfunding (Reuters and Thompson 2017).

³⁵ Without a 3G or 4G, consumers can't access the internet.

³⁶ Cloud computing requires access to reliable, high-speed infrastructure at a reasonable price and is critical in reducing costs for fintech startups and SMEs as well as they scale up.

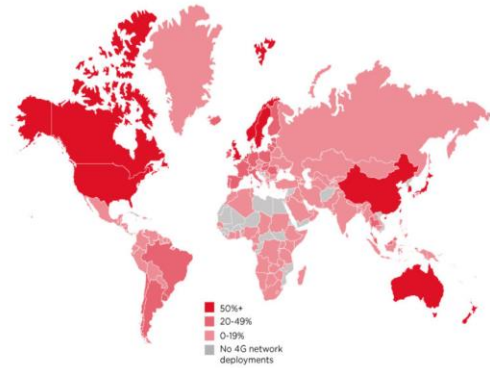
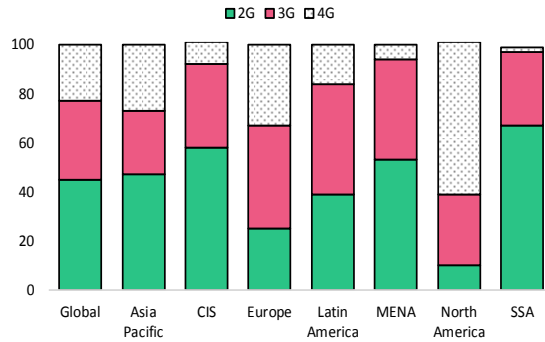
³⁷ In some countries (Somalia), there are reports of agencies running out of cash which can affect trust in mobile payments.

Figure 15. State of the ICT, Payment System, and Credit Evaluation Infrastructure

Deployment of high speed networks is comparatively low ...

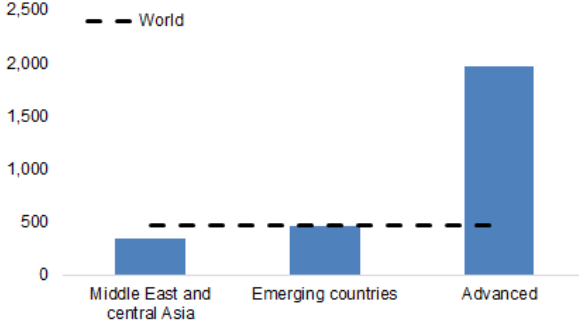
...and 4G coverage is uniformly low in MENAP and CCA

Technology Mix, 2016

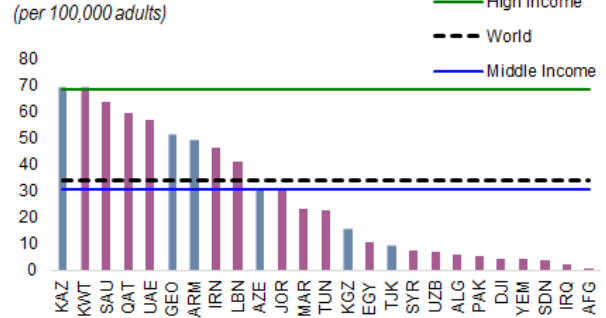


POS and ATMs that play an important role in "cash in and out" and which is critical for financial inclusion is lagging

Point-of-sale terminals (per 100,000 adults)

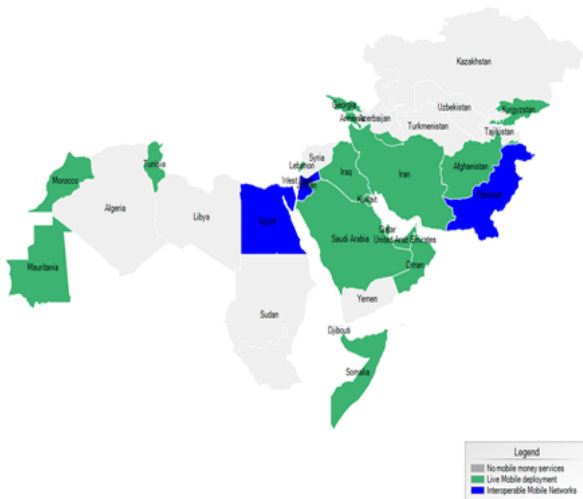


Automated teller machines (ATMs) (per 100,000 adults)



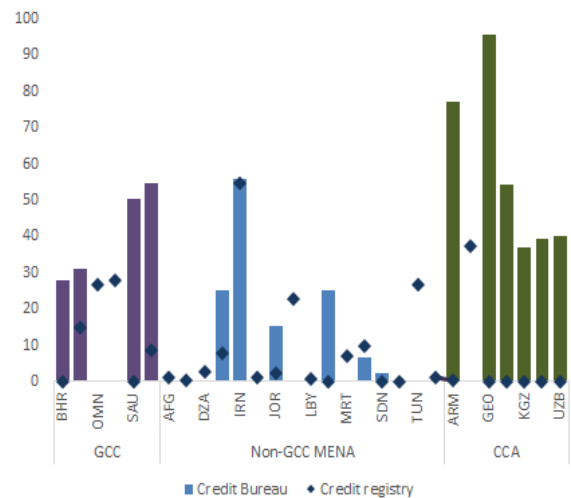
Source: IMF Financial Access Survey.

Few countries have interoperable systems which results in market fragmentation



Infrastructure for credit risk evaluation is weak in many countries

Credit Bureau and Registry (Percent of Adults)



Source: GSMA and World Bank Doing Business

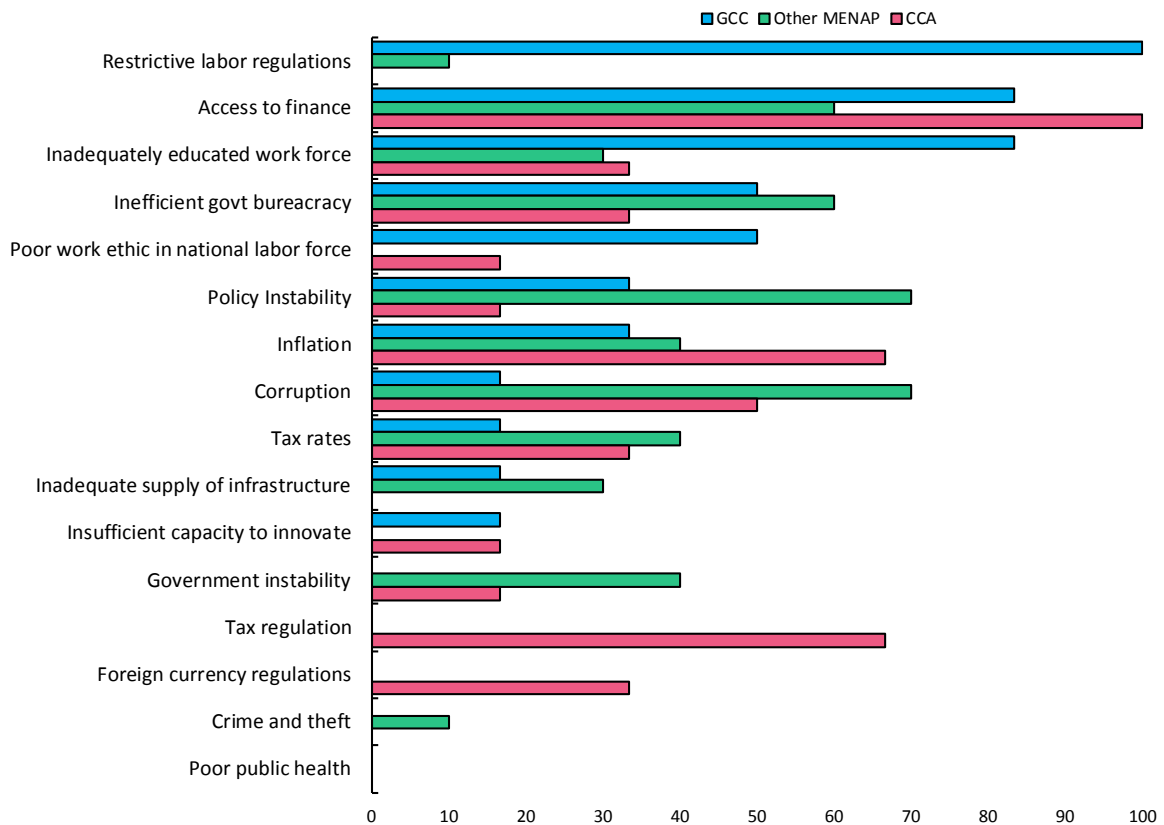
The overall business environment remains restrictive for innovative new entrants

(Figure 16). In the GCC, companies identify restrictive labor regulations, access to finance, skill gaps, work ethics, and inefficient government bureaucracy among the top five challenges. Given the limits on foreign shareholding coupled with weaknesses in regimes to protect minority shareholders, investors may be unwilling to invest capital or establish a presence in the absence of a trusted local partner or network.³⁸ In other MENAP countries, firms cite policy instability and corruption in addition to access to finance and government bureaucracy. Unreliable electricity supply, alluded to earlier, also remains a significant problem for firms in some countries. In the CCA, firms rank access to finance as a major constraint but also give prominence to inflation and tax regulation.

Figure 16. Factors Adversely Impacting the Business Environment

Problematic Factors for Doing Business

(Percent of countries identifying the constraint among the top five)



Source: WEF, Global Competitiveness Report 2017-18

Note: The following countries are excluded in the aggregates due to lack of information: Iraq, Afghanistan, Djibouti, Sudan, Syria, Turkmenistan and Uzbekistan

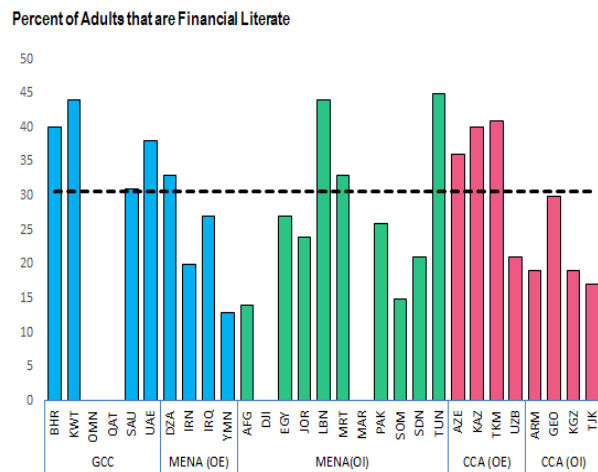
A broad range of demand factors also constrain fintech’s growth potential. These in the main include lack of trust, low financial literacy, entrenched effective informal mechanisms, low income levels, data security concerns, and cyber security fears. Fintech innovations in MENAP face a big “trust gap,” which has forced them to seek collaboration with banks (WAMDA 2016).

³⁸ The UAE and Qatar only permit a non-national or non-GCC shareholder to hold 49 percent of a company.

Uptake of mobile payments is, in some countries, also constrained by low financial literacy levels and while the effectiveness of the informal Hawala system in the remittance markets of both the MENAP and CCA also presents an important hurdle to the adoption of mobile payments. In some countries (Armenia, Djibouti, Georgia, Iraq, Kyrgyzstan, and Somalia), the cost of internet and mobile services relative to income limits demand for digital financial services.³⁹ There is also still a great preference for cash on delivery in e-commerce transactions, due to concerns about security of online payments⁴⁰ (Figure 17). The lack of awareness and small market has also been cited as a major constraint in crowdfunding scaling up in Kazakhstan.

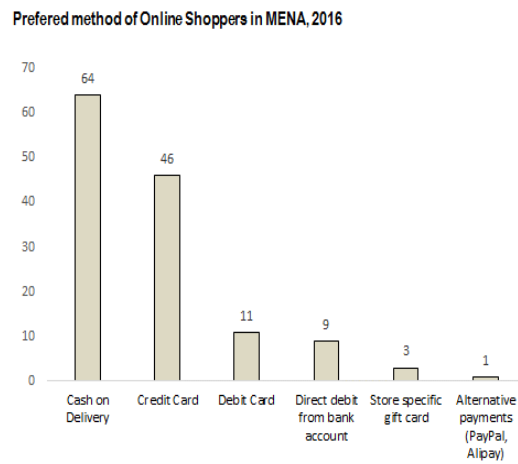
Figure 17. Customer Preferences and Literacy Levels

Financial literacy levels remain low in some countries



Source: SSP Global Financial Literacy Survey

The preference for cash on delivery could delay digitization



Source: Statista and Clixgroup, 2017

Data and cyber security concerns delay broader adoption of some technologies, such as cloud computing. Data security is a concern held strongly in the MENA region and this has implications for start-ups that cater to government organizations and large corporates, because these clients have strict regulations with respect to where their data is stored. Concerns over third-party cloud computing and storage providers, data sovereignty and security, the lack of cloud related regulations and national cloud strategies have thus slowed the adoption of public clouds in many MENA countries, including the GCC. Banking sectors in MENAP have also been slow to adopt some of the technologies (cloud computing and big data analytics) due to migration costs of shifting from legacy system architecture as well as concerns about their capacity to implement advanced security solutions and to remain compliant with local regulations, including data sovereignty rules for the finance industry [Thompson Reuters 2017].

³⁹ A mobile plan costs more than 10 percent of incomes for over 80 percent of the population in Armenia, Georgia, and Kyrgyz Republic (World Bank 2017c). In Somalia and Djibouti, less than a third of the population subscribe to mobile networks. Most networks are also still 2G, thus limiting internet adoption.

⁴⁰ While in Dubai electronic payments are part of the landscape, in other countries (such as Egypt) cash on delivery is the principal method.

Innovations have focused more on the low hanging fruits of improving services for the banked population and less on enhancing financial inclusion. Current fintech innovations in the MENA and CCA regions have focused on retail payment instruments, such as electronic wallets (e-wallets) that are sometimes linked to cards and mobile phones and can be used as a form of payment, to withdraw cash, to pay bills, recharge airtime, make deposits, and send or receive money transfers. Innovations that have potential to improve financial inclusion or SME access to finance, such as mobile financial services for unbanked populations, Reg Tech (credit scoring, risk management, and regulatory compliance) trade processing, Market Place Lending (MPL) and crowdsourcing are either in the nascent phase or are yet to emerge. Indeed, McKensie’s digitization index shows that the MENA has yet to satisfy full potential, especially in business and government.

Socio-economic and political factors constitute major constraints in selected countries. In MENAP, poverty, the high cost of internet relative to income, high cost of using financial services, and financial illiteracy also limit development of fintech and increased the potential gap in the adoption of mobile financial services in some countries (Afghanistan, Djibouti, Somalia, Pakistan). Fintech innovations will also need to be made Sharia’h compliant if the products are to be widely adopted across all segments. Thus far, initiatives to develop Sharia’h compliant fintech products are in early developmental phases.⁴¹ In the CCA, too, mobile costs remain prohibitive in many countries (Armenia, Georgia, Kyrgyz Republic).⁴²

IV. FINTECH: A VALUE PROPOSITION FOR THE MENAP AND CCA REGIONS

Fintech presents important opportunities that are in line with the MENAP and CCA regions’ macroeconomic priorities. Both regions have placed economic diversification and inclusive growth at the heart of reforms, and financial inclusion of unbanked populations and improved access to SMEs are the vehicles through which the broader objectives are to be attained. In the aftermath of the decline in oil prices, after 2014, fiscal consolidation and improving efficiencies in government operations also assumed great importance. Transparency and reducing corruption are also emerging policy priorities and, more recently, concerns have focused on the withdrawal of cross-border banking operations. Fintech can help countries achieve many of these policy goals.

A. Inclusive Growth

Fintech has potential to promote financial inclusion and the broader objective of inclusive growth in the MENAP and CCA through a variety of channels. For both regions, fintech can facilitate access to financial services for unbanked populations and underserved SMEs, create jobs commensurate with digital age millennial populations, improve government operations, and reduce the informal economy. The relative importance of these channels, however, varies across

⁴¹ In December 2017, the consortium consisting of the three Bahraini banks launched a new company named ALGO Bahrain with a vision to drive research and development in the Islamic-compliant FinTech sector.

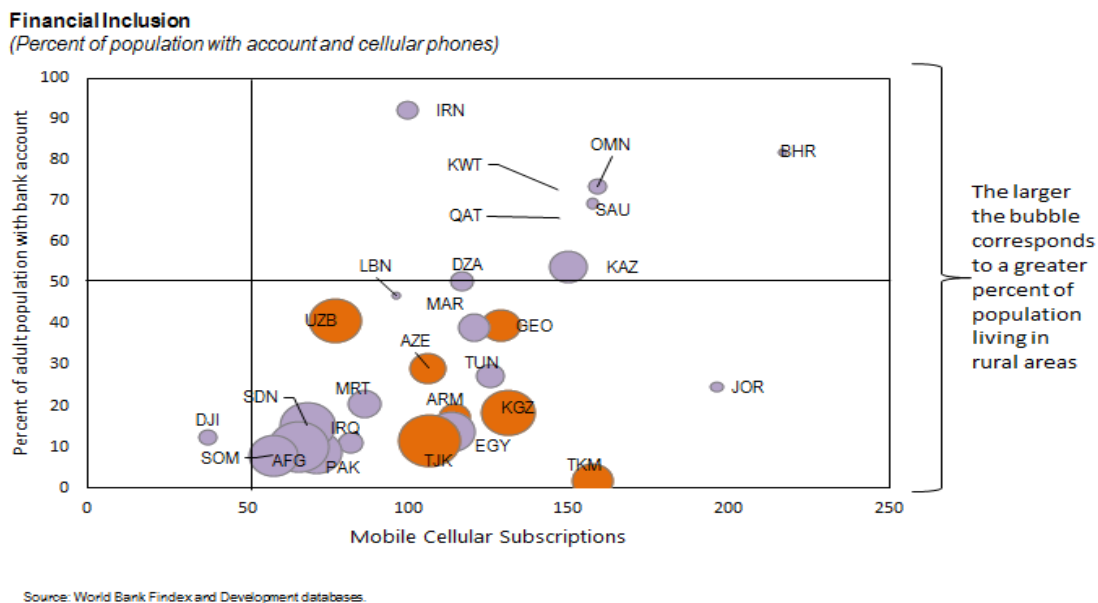
⁴² See footnote 39.

countries because of the diversity in demographics and levels of bank access, internet, and mobile phone development.

Mobile financial services can be a game changer in facilitating financial inclusion in the MENAP and CCA, if appropriate regulations are put in place and infrastructure constraints are alleviated. Mobile penetration rates exceed the number of bank deposits in more than half the countries in MENAP and have penetrated rural areas where low density populations discourage bank branches (Figure 18). These metrics are even more pronounced in the CCA where more than 60 percent of the population live in rural areas and are mostly unbanked as the challenging topography makes bank penetration in rural areas difficult.⁴³ However, some countries (Djibouti, particularly but also Afghanistan, Pakistan, Somalia and Sudan) with low mobile penetration will require additional investments in ICT infrastructure, in addition to putting in place enabling regulatory frameworks.

Figure 18. Unbanked populations and Rural Urban Divide

*In most countries, mobile penetration exceeds access to bank accounts.
..and many countries with low access also have high rural populations*



⁴³ In the GCC, over 70 percent of the adult population have bank accounts, smartphone penetration is among the highest in the world, credit and debit card penetration is also high, and rural populations are small with only about 20 percent of populations living in rural areas so mobile banking tend to serve the banked populations.

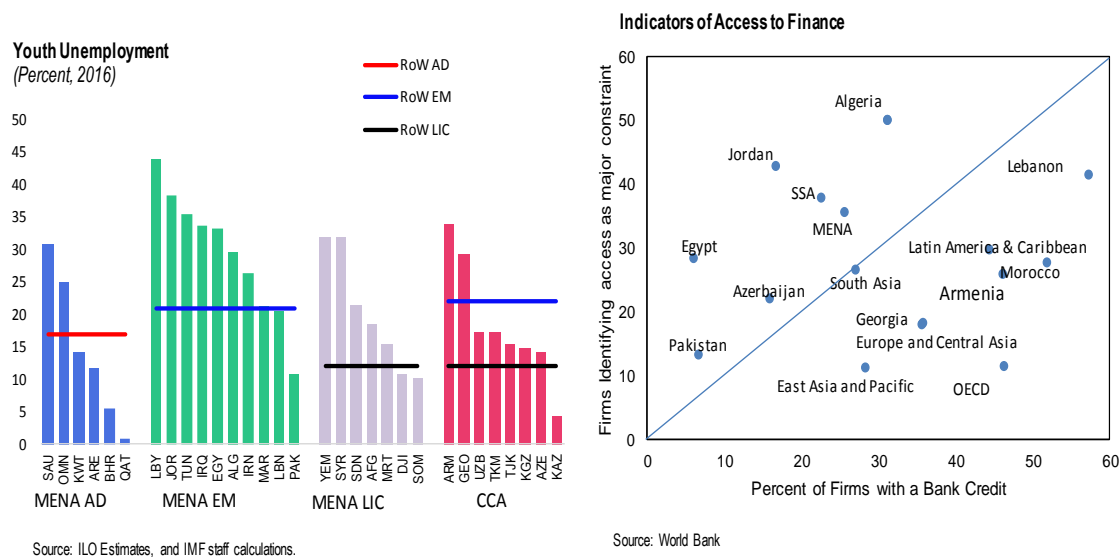
But there is great diversity across subregions in the potential for mobile payments to increase financial inclusion

CROSS COUNTRY ANALYSIS OF PROSPECTS FOR MOBILE FINANCIAL SERVICES (MFS) DEVELOPING				
DEMAND FOR MFS	PROSPECTS	COUNTRY	DRIVERS	IMPEDIMENTS
MENAP				
VERY HIGH	VERY HIGH	Egypt, Morocco	<ul style="list-style-type: none"> • High levels of unbanked populations • High rural populations • Conducive regulatory regimes • Financial inclusion a priority in the national agenda • High mobile penetration • Interoperable mobile networks in Egypt • Morocco passed banking law to allow nonbanks offer payment services 	<ul style="list-style-type: none"> • For Egypt, the requirement that MNOs operate only through banks could inhibit innovation
VERY HIGH	HIGH	Afghanistan, Pakistan, Sudan, Somalia	<ul style="list-style-type: none"> • High levels of unbanked people • High rural populations • Financial inclusion is part of the national agenda 	<ul style="list-style-type: none"> • Mobile penetration less than 70 percent so additional investment in ICT would be needed to scale up mobile financial services
VERY HIGH	MEDIUM	Algeria, Iraq	<ul style="list-style-type: none"> • High unbanked populations (more than 50-90 percent of the adult population) • Close to 30 percent of population is in rural areas 	<ul style="list-style-type: none"> • High state ownership and control of banking and telecom sectors • Uncertain regulatory and business environments
LOW	HIGH	Saudi Arabia, Kuwait, Bahrain, Oman, Qatar, UAE, Iran	<ul style="list-style-type: none"> • High mobile, internet and smart phone penetration 	<ul style="list-style-type: none"> • Incentives are low since unbanked populations are < 20 percent • Small rural populations • Uncertain regulatory and business environments
VERY HIGH	LOW	Djibouti	<ul style="list-style-type: none"> • High levels of unbanked populations 	<ul style="list-style-type: none"> • Low mobile penetration thus further investments in ICT infrastructure are needed to scale up mobile financial services • High state ownership and control of banking and telecom sectors
CCA				
VERY HIGH	MEDIUM	Armenia, Azerbaijan, Georgia, Kyrgyzstan, Tajikistan, Uzbekistan,	<ul style="list-style-type: none"> • High unbanked populations (more than half the adult population) • High rural populations (between 40-70 percent of the population live in rural area) • High mobile penetration (between 70 percent and 155 percent) 	<ul style="list-style-type: none"> • Uncertain regulatory and business environments

Fintech can reduce SME funding constraints and generate employment that reduces income disparities and promotes growth that is inclusive. SMEs in MENAP and CCA, respectively, account for between 80 percent and 95 percent of formal sector enterprises and about 50 percent of employment, but their growth is constrained by limited access to finance (Figure 19), which in turn is related to poor accounting records, lack of collateral, and the absence of financial products tailored to SME needs.⁴⁴ Predictive analytics using big data can enhance banks' abilities to assess SMEs' creditworthiness and unlock the credit for SMEs. Digital payments create a data trail for SMEs that enables banks to lend to SMEs against cashflow. DLT can provide superior record-keeping for collateral registries that facilitates collateral based lending. Moreover, crowdfunding and Market Place P2P lending platforms can provide alternative funding sources, including through foreign platforms.⁴⁵

Figure 19. Unemployment Levels and SME Access to Finance

Unemployment is high in the MENA and CCA but growth of SMEs that can help create jobs by limited access to finance



Fintech firms can also be a direct source of job creation and growth, if appropriate skills are developed. The MENAP and CCA regions have some of the highest levels of youth unemployment in the world. In several countries—Libya, Saudi Arabia, West Bank and Gaza, Iraq, Tunisia, Jordan, Egypt, Syria, and Yemen—youth unemployment ranges between 30–50 percent. Technology start-ups provide employment opportunities in many sectors (IT software, data analytics etc.) suitable to digital age millennial populations and can act as the backbone of the region's economy, driving growth, productivity, diversification, and job creation.

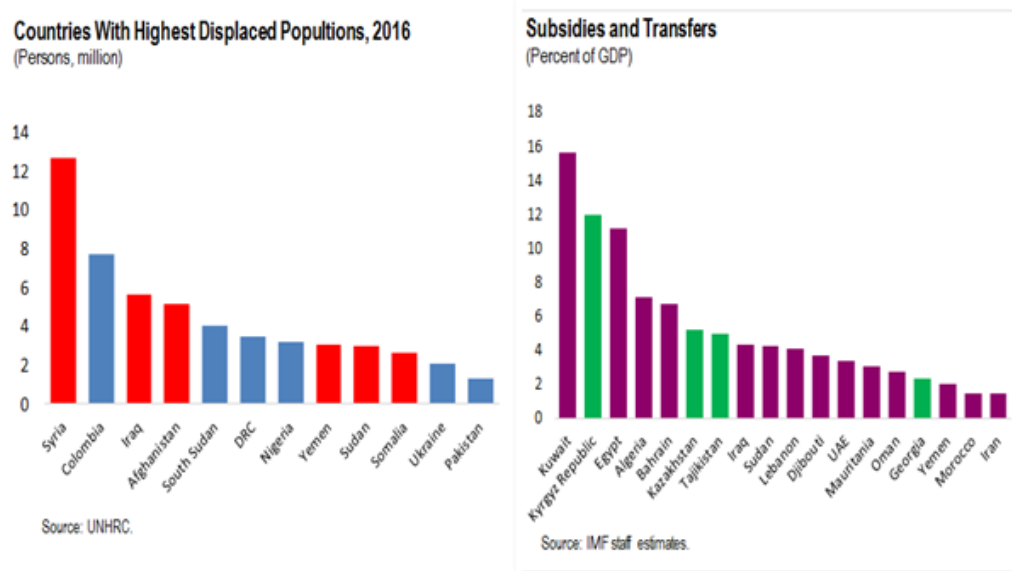
⁴⁴ See Lukonga 2014 for an elaborate discussion of the funding challenges that SMEs face.

⁴⁵ Equity crowdfunding integrates well with Islamic culture.

Digitization can also facilitate efficiencies and transparency in government operations and support humanitarian efforts and initiatives to tackle corruption. The MENA is home to the highest number of displaced persons due to ongoing disputes in countries such as Iraq, Yemen, and Syria that have led to mass migration to Jordan, Lebanon, and Egypt (Figure 20). Mobile payments can facilitate social transfers in a manner that preserves human dignity.⁴⁶ More generally, digital payments make government transactions transparent and auditable, which can help reduce corruption and fraud. Indeed, several countries (Afghanistan, Oman, Pakistan) are already leveraging e-payments for government payments and social transfers.⁴⁷ In the CCA, several countries (Kazakhstan, Azerbaijan) have shifted to automated online payment systems for government revenue collection.⁴⁸

Figure 20. Displaced Populations and Social Transfers

The MENA has large displaced persons... ..and social transfers are substantial



Fintech can improve efficiencies in cross-border remittances and help reduce the informal sector. The MENAP and CCA regions have large migrant populations that have made them major inward and outward remittance corridors and remittance costs in the region remain high (Figure 21). Cash transfers and slow and costly bank transfers are traditionally the principal channels for making remittances. Fintech innovations (P2P transfers, DLT) can facilitate faster and

⁴⁶ In 2016, humanitarian organizations effectively used mobile money to digitize Jordan cash transfers in response to multiple displacement crises in Iraq, Afghanistan and Pakistan.

⁴⁷ In Afghanistan, mobile payments have facilitated greater transparency and reduced corruption in the payment of government salaries. Before the deployment of mobile payments, middlemen used to siphon as much as 30 percent of salaries to police. Mobile wallets can also replace cash in countries like Iraq where moving cash poses logistical as well as security problems.

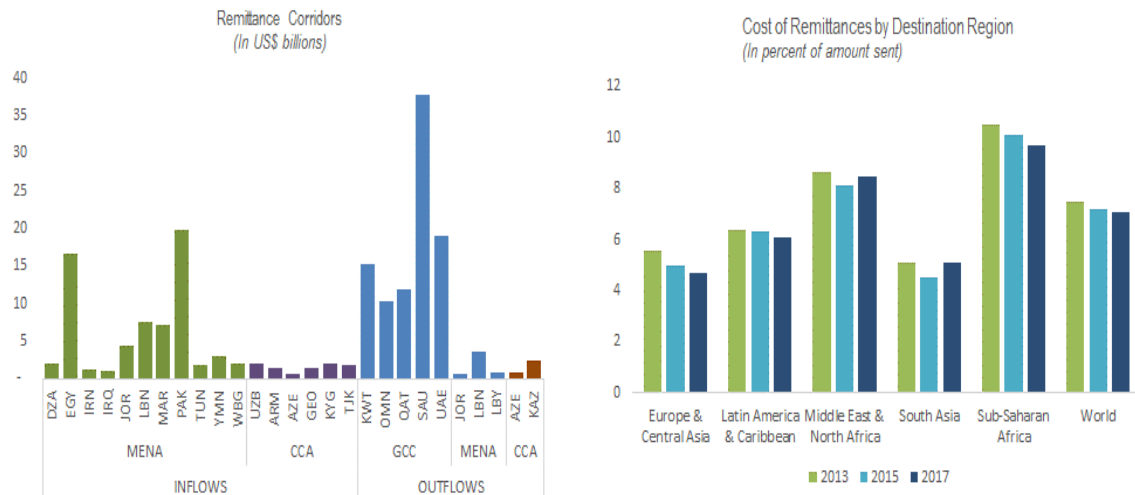
⁴⁸ Kazakhstan government partnered with a processing company to bring greater efficiencies through the "One click payment" which allows you to pay for the services without re-entering your payment card details.

lower cost remittances. Moreover, as many migrants are excluded from banking services, fintech can attract remittances into the formal financial sector.

Figure 21. Remittances Volumes and Transfer Costs

The MENA and CCA have major inward and outward remittance corridors

But remittances costs remain high



Source: World Bank Remittance Price World Wide

B. Financial Stability, Integrity and Financial Inclusion

Fintech can support financial stability by reducing banks’ operational costs and improving risk management. The same technologies that offer efficiencies and opportunities for fintech firms and banks, such as AI/advanced data analytics, DLT, cloud computing and APIs, can automate processes and improve risk management in banks as well as improve supervisory efficiency and effectiveness. Credit scoring using predictive analytics can augment data on credit registries which are currently weak. With few exceptions (Armenia and Georgia) coverage of credit registries remains low across the two regions and some countries are yet to establish credit registries. Improvements to banks credit risk management can unlock bank credit without weakening asset quality.

Fintech can also improve financial integrity, support financial stability and financial inclusion, and possibly contribute to solutions for declining Correspondent Banking Relationships (CBRs). Concerns with respondent banks’ ability to manage AML/CFT risks and the potential sanctions for noncompliance coupled with profitability concerns have led to the withdrawal of CBRs in several countries (Djibouti, Sudan, Somalia and Kyrgyzstan).⁴⁹ The

⁴⁹ Even some big regional banks have registered declines in CBRs.

withdrawal of CBRs has negative effects on trade, growth, welfare, and financial inclusion,⁵⁰ while the fight against financial crime has increased regulatory compliance costs. To avoid losing CBRs, banks need to improve processes and controls to meet international standards and to have clear and auditable systems. Financial technologies (big data, blockchain, and identify technologies) can facilitate regulatory compliance, enable P2P transfers that reduce reliance on CBRs, and reduce the costs and lengthy process of CDD and KYC requirements. The adoption of technology for regulatory compliance (RegTech) in the two regions is still very much work in progress but some countries (UAE) have begun to organize regional conferences to explore its potential and current constraints to adoption.

V. UNLOCKING THE TRANSFORMATIVE POTENTIAL OF FINTECH

Fintech holds great promise to foster inclusive growth in the MENAP and CCA if the relevant regulatory and logistical frameworks are put in place and structural constraints are addressed. Policy initiatives already taken are encouraging but more is needed to ensure that regulations do not stifle innovation and financial stability and security risks are mitigated. Fintech innovations also vary in their macro-financial impact so a strategic approach is needed to ensure that incentives are designed in a manner that aligns fintech innovations with the regions' policy priorities of financial inclusion, economic diversification, reducing corruption, financial stability, and integrity.

A. Promoting Innovation while Safeguarding Financial Stability

The sound development of fintech requires a multi-pronged policy strategy. The policy priorities vary across countries reflecting the differences in the stages of fintech development and the policy and institutional environment, but the general areas warranting immediate attention are measures to mitigate cyber risks, update the financial, legal, regulatory and supervisory frameworks, and easing demand constraints.

Cyber security should be a top policy priority. Cyberattacks have potential systemic financial stability risks and can discourage adoption of fintech, thus there is an urgent need to develop comprehensive cybersecurity frameworks that include prevention, detection, information sharing, monitoring, financial and technology literacy, and recovery plans. Regulatory oversight should ensure that banks and other financial institutions have cybersecurity throughout the payments chain, including with merchants who are operating as agencies. Investments in technologies that prevent cybersecurity should be accompanied by training programs to increase awareness by staff, to prevent weak links which cybercriminals can exploit. New technologies should integrate security measures into their design.

Legal amendments may be needed for some countries to provide clarity and certainty to fintech transactions and the licensing requirements. Greater reliance on regulations and

⁵⁰ It increases the cost of remittances, has led to domestic banks (Kuwait, UAE, Bahrain) severing relations with SMEs and remittance companies for fear of potential sanctions for non-compliance with AML/CFT, and encourages the migration of remittances into informal channels.

guidelines can facilitate a dynamic regulatory architecture that can address risks as they emerge in the fast-changing landscape, but laws need to give the powers that set the basis for implementing regulations. A review of legal and regulatory frameworks against the emerging fintech market structure can help identify gaps and restrictions in the law and regulations that hamper innovation and can enable development of a comprehensive and systematic roadmap for reforms. Regulatory sandboxes can facilitate better understanding of risks posed by fintech firms and enable appropriate design of regulations.

Gaps in prudential regulations warrant attention. A functional and proportional approach to regulation can help level the playing fields, as well as ensure that innovations do not fall outside the regulatory perimeter and that regulation does not stifle innovation (Dong and others 2017). Payment regulations should provide clear guidelines governing operations of electronic money institutions. *Virtual currencies* should be regulated to prevent money laundering and financing of terrorism, and their dynamic and uncertain legal form require cross-border cooperation (IMF 2017). For crypto asset exchanges, the regulatory framework should, in addition to integrity issues, address consumer protection, technology governance, and safe custody. Equity crowdfunding and other online platform lending requires prudential and conduct of business regulations that are underpinned by strong protections for depositors, minority shareholders, and strong insolvency regime. Regulations governing outsourcing risks should be adapted to cover emerging innovations, such as cloud computing, and should require ongoing monitoring, appropriate contingency plans, and regulatory authority to examine third parties.⁵¹

Supervisory frameworks and capacities will need aligning with the evolving financial landscape. Central banks and financial regulators need to upgrade their expertise and internal control mechanism, including operational risk management. Reporting requirements for licensed entities should be developed to enable supervisors monitor changes in market structures brought about by fintech, facilitate risk identification, monitoring and timely policy response. The licensing tool should be used to ensure that fintech firms have effective systems and controls.⁵² Supervisory reviews should begin to cover cyber risk preparedness, risk management practices of banks vis-a-vis third parties, concentration risks in third party providers, and IT risks and ensure that new technologies do not become tools for fraud, money-laundering, and terrorist-financing. Collaborative arrangements between the financial regulator and other nontraditional regulatory agencies will need strengthening.⁵³ Since cyber security is not location dependent, and as some

⁵¹Regulations should give regulators statutory authority to examine third party service providers who have contractual relationships with regulated financial institutions, and also require ongoing monitoring and appropriate contingency plans.

⁵² Six areas that warrant attention at the licensing stage including IT security/fraud, reliability and business continuity, business risk, contractual relations and enforceability, use of third party agents, credit and liquidity risks to customers as account holders.

⁵³ These include regulators for telecommunications, competition authorities and consumer protection, if the latter is not within the mandate of the prudential regulator.

of the fintech firms have cross-border operations, cross-border collaboration is needed. Compliance with international standards should be enforced.⁵⁴

Demand factors also require attention. These include financial literacy programs and strengthening consumer protection frameworks to improve trust. Digital products offered through mobile instruments provide a solution to the physical inaccessibility to financial institutions. However, availability is not a sufficient condition to ensure usage, thus, greater efforts should be made to increase the awareness and competence needed to improve uptake and usage of digital financial services. Strengthening consumer protection frameworks could improve trust and confidence in fintech innovations, and also facilitate uptake and usage of digital financial services. This requires strengthening regulations governing data and privacy laws and management of consumer funds in “stored value facilities”. Liquidity guidelines should be considered to ensure that payment service providers have adequate liquidity to readily meet customer demands.

B. Aligning Fintech with Policy Priorities

Not all fintech innovations add economic value, thus a strategic approach to the development of the fintech industry is needed. Although the internet and hand-held devices are ubiquitous in the MENAP and CCA, they are mostly used for accessing social media, rather than for business. Digital economic sectors remain nascent and entrepreneurial potential is yet to be fully tapped. The incentive structure should, therefore, be designed in a manner that promotes innovations with higher economic values, thereby aligning fintech growth with the regions’ macro priorities of financial inclusion, economic diversification, and the broader objective of inclusive growth. There is also a need for medium-term structural reforms to address gaps in infrastructure as well as capital, and talent while further strengthening the business environment.

Regulatory reforms should be designed to create a competitive environment and ease impediments to financial inclusion. One basic requirement is to allow nonbanks to offer mobile financial services and issue e-money while ensuring appropriate safeguards are in place to protect consumers and there is oversight to ensure sound institutions. Interoperability should be promoted to reduce market fragmentation, but this should be encouraged without mandating it. Regulations should allow agency networks to facilitate banks invest in POS infrastructure that facilitate financial inclusion.

Public private partnerships could be useful in aligning fintech with policy priorities. Hackathons to promote innovations that come up with market solutions to ease SME access to

⁵⁴ The CPSS-IOSCO and General Principles for International Remittance services can, respectively, provide a general framework for assessing risks and providing oversight for mobile payments. Guidance for a risk-based approach, prepaid cards, mobile payments and internet-based payment services of 2013 is also useful. The FATF recommendations support the development and implementation of a risk-based approach to AML/CFT.

finance such as creating digital financial accounts, improve credit reporting systems, and collateral registries for moveable collateral should be encouraged.

Structural constraints will need to be addressed in a comprehensive and well-sequenced medium-term reform programs. Focus areas of relevance to fintech are the gaps in infrastructure, capital, and talent together with the overall business environment.

- The quality of infrastructure is critical in unleashing fintech innovations. This requires ensuring that electricity is widely available, deregulating ICT sectors to enable competition, investing in fiber optics to ensure that ICT *at least* include 3G and are affordable, and modernizing the payment system infrastructure. There is also a need to strengthen the credit infrastructure framework, including credit reporting systems (CRS), secured transaction and collateral regime (STCR) and insolvency regime to reduce the information asymmetries and legal uncertainties that increase risk to lenders and constrain the supply of finance to SMEs.
- Factors constraining *private equity and venture capital* should be identified. In this context, restrictions on foreign investment could be eased to increase the availability of capital as well as enable entry of established Fintech companies.
- Reforming insolvency laws will also reduce legal uncertainties that increase risk to lenders and constrain the supply of finance.
- *Talent gaps* in many countries point to the need for education reform to equip new graduates with skills necessary to operate in digital economies as well as reforms of work permit system to augment domestic talent.

Overall, expediting these reforms can ensure that the MENAP and CCA regions are not left behind. Fintech is emerging from the gaps into the mainstream of the financial services ecosystem and customer expectations are rapidly changing. Harnessing emerging digital technologies is, therefore, critical for financial institutions to meet customer needs as well as enable policy makers achieve some of the policy priorities, such as achieving efficiencies in government operations, financial inclusion and the broader objective of inclusive growth. The sound development of fintech will, however, require a careful sequencing of policies to ensure that regulations do not stifle innovation, risks are adequately mitigated and customer confidence is maintained.

Box 1. Cross Country Experiences with Fintech

Cross country experiences demonstrate that with appropriate regulations, fintech innovations in payments and lending can promote financial inclusion and enhance SME access to finance. The experiences also underscore the dynamic and multi dimension sources of cyber risks and the threats.

United States (US)	The US has fintech companies across the spectrum of financial services. Growth of fintech has been underpinned by high-quality infrastructure, abundant talent and availability of seed, venture and growth capital. Government support has been limited and the regulatory uncertainty due to the mixture of multiple federal and state regulators is cited by the industry as a dampening factor to the growth of fintech. Marketplace lending firms (Zopa, Lending Club and Funding Circle) registered rapid growth in online lending, but weak governance, poor internal controls and asset quality problems eventually plagued some of them. State-of-the-art technical measures for cybersecurity have been developed but cyberattacks have resulted in customer data breaches. Misuse of data from Facebook by Cambridge Analytica underscores the data privacy risks.
United Kingdom (UK)	The UK has a well-developed fintech industry underpinned by favorable government and regulatory support under the 'Project Innovate' program that includes an innovation hub and regulatory sandbox. The crowdfunding ecosystem is developed with clear regulations on transparency and consumer protection, including setting minimum capital standards and requiring firms to have resolution plans in place, ensuring that loans continued to be repaid even if the platform collapses. Banks are also required to direct small businesses to alternative finance providers if they can't fulfill their financing needs themselves. As a result, the market share of "digital first, mobile only" banks ("challenger" banks) and alternative finance providers jumped from 4 percent in 2012 to 12 percent in 2014 (Ernst and Young 2016a). Prudential oversight of market place lenders (P2P) also enabled significant credit growth through lending platforms while concurrently containing credit risks. The U.K. has also invested significantly in cybersecurity, but the recent "wannacry" cyber-attack exposed vulnerabilities in several financial and non-financial companies.
China	In China, the fintech industry has grown rapidly underpinned by rapid growth in e-commerce growth, online and mobile penetration, large unbanked populations, lax regulations and easy access to capital. P2P lending platforms significantly increased funding for unbanked individuals and SMEs. However, some platforms did not invest the funds raised in intended SMEs but joined the surge on the Chinese stock market only to be driven into bankruptcy when the market collapsed. These circumstances ultimately led to the Ezubao scandal in 2016 in which almost 1 million investors lost US\$7.6 billion through a Ponzi scheme. China has introduced more rigorous cyber security laws in the aftermath of the global "wannacry" ransomware attack that affected some bank operations (Ernst and Young 2016b)
Kenya	The M-Pesa model in Kenya has been very successful in achieving financial inclusion through deployment of mobile technology, reaching 80 percent of households within four years (World Bank 2016). The Central Bank of Kenya adopted a functional, rather than an institutional, approach to regulation where banks and nonbanks, including mobile network operators, are permitted to provide mobile money services.

Box 2. Infrastructure for Digital Financial Inclusion

ICT Infrastructure	The ICT infrastructure should facilitate connectivity thus higher broadband such as 3G, 4G and 5G is needed (fixed infrastructure and data centers). G2 does not enable internet
Payment System	The payment system needs to be interoperable to avoid market fragmentation and also facilitate real time settlements to enable meeting payment deadlines.
Credit Information	Credit information infrastructure should be designed to provide information on debt and delinquency to enable providers to assess risks of counterparties and thereby help providers increase the rate of access to bank financing and to lower costs of credit.
Agency network	PoS and agents are also crucial and distinguishing assets of mobile money providers because of the need for cashing in and out.
Energy Authentication	A reliable supply of electricity is needed to enable internet to operate Fintech products are predominantly web based, thus fintech companies face the challenge of legal identification and legitimation of (potential) customers to avoid any sort of illicit activity or a data breach

Box 3. Cyberattacks Impacting Financial Institutions in MENAP and CCA, 2012–2018

In tandem with global trends, the volume of threats in the MENAP and the CCA have continued to increase and the threat landscape has become more diverse. Thus far, the cyber incidents have included hacking through third parties, compromising the ATM infrastructure, banks computer systems, websites and other data breaches.

Hacking through third party vendors: In 2012 and 2013 cyber criminals hacked into two card processing centers in India that handled payment processing of prepaid cards for a bank in Oman and another in the United Arab Emirates. The cybercriminals increased available balances and withdrawal limits on prepaid debit cards as well as coded fake cards that enabled them to withdraw US\$45 million from ATMs in 27 countries.

Compromising ATM infrastructure: In 2016, cybercriminals used special malicious software to force ATMs dispense cash in Armenia, Georgia, and Kyrgyzstan. and UAE. The UAE was a target several cyberattacks including ATM skimmer malware, targeted is the core of the ATM, which is responsible for interaction with the wider bank infrastructure, card processing and dispensing of cash enables cybercriminals to capture data – including a customer’s bank account number and PIN - from the cards used at the ATM or steal cash directly

Compromising banks computer systems: Using malicious e-mails to spread hacking programs, in 2017, cybercriminals infiltrated bank computers in Armenia and stole valuable data on customers and bank accounts, resulting in losses amounting to 133 million AMD (approximately US\$273,000). In 2017, cybercriminals hacked the computer system of an Azerbaijani bank resulting in financial losses of 3.7 million manats (\$2 million).

Denial of service: In 2012, cybercriminals hacked into and disrupted websites of several financial institutions, including the Abu Dhabi Securities exchange, Saudi Arabia exchange, UAE central bank websites and the Arab Bank Palestine. In 2015, Azerbaijan Central Bank website was defaced and customer data was stolen.

Data breaches: In 2015 cybercriminals hacked into a UAE bank and demanded ransom to be paid in digital currency (Bitcoin) by leaking confidential financial transactions and client details on social networking. In 2016, one of Qatar’s largest banks suffered a data breach involving client information.

Glossary of Terms	
Agent network	A collection of businesses, such as retailers, with which a bank or other financial services provider contracts to serve as points of interaction with the provider's customers.
Cash-in, cash-out	Transaction to convert a balance in a transaction account into cash, or incrementing a balance by paying in cash.
Digital (financial) services provider	A mobile network operator or other nonbank entity that offers various financial services but only by electronic means, for example, using a mobile phone or the Internet.
E-money	A record of funds stored on a payment device, such as a chip, a prepaid card, or a mobile phone, or on a computer system as a nontraditional account with a banking or a nonbanking entity. E-money products can be further differentiated into network money, mobile money, electronic purse, and electronic wallet (e-wallet).
E-wallet	An e-money product for which the record of funds is stored on a specific device, typically a chip on a card or in a mobile phone.
Float.	The aggregate of funds that, for a short interval after a transaction, have been credited to the account of the recipient but not yet debited from the account of the sender.
Functional approach	An approach to financial services regulation in which services of the same nature are regulated in the same way, rather than, for example, according to the type of provider.
Interoperability	In mobile money markets, interoperability implies the ability of users of one network to transact with users of another network, which can be achieved at different levels—at the customer level, at the agent level, or at the platform level.
Know-your-customer (KYC) regulation	Government rules and regulations that require a financial services provider to exercise due diligence in establishing the identity of its users, specifically, to ensure that the user is not engaged in money laundering or terrorist financing.
Mobile money	An e-money product for which the record of funds is stored on a mobile phone
Mobile network operator.	A provider of wireless communications services that owns or controls the infrastructure necessary to deliver those services.
Person-to-person transfer (P2P)	A transfer of funds directly from one person to another by electronic means rather than by cash or check.
Point of sale (POS)	The place at which a retail transaction is completed by the customer making a payment to the merchant, using traditional or digital means, in exchange for goods or services.
Risk-based approach.	An approach to financial services regulation that follows the principle of proportionality, such that the stringency of regulation of an activity is commensurate with the risk that the activity poses to users and creditors or to the system as a whole.
store-of-value instrument.	An account such as a deposit account, or an account on a device such as a magnetic card, that contains negotiable monetary value for a period longer than is necessary to complete a transaction.

References

- Aboul-Enein Sameh. 2017. Geneva Center for Security Policy (GCSP). 2017. Cybersecurity challenges in the Middle East. 22/17 Research Series.
- Ali Rouda Al Amir. 2016. Cloud Computing in Arab States: Legal Aspects, Facts and Horizons. ITU-ATU Workshop on Cybersecurity Strategy in African Countries. Khartoum, Sudan 24–26, July 2016. Program Officer. ITU Arab Regional Office.
- Al Tamimi and Company. 2017a. MENA Cloud Alliance launches GCC Cloud Competitiveness Index 2017
- Al Tamimi and Company. 2017b. Setting up in the Dubai International Financial Centre
- Morgan Lewis. 2016. New Kazakhstan Law on Payments and Payment Systems: Key Novelties Article by Nurgazyeva A Klara and Mukhamediyev Marat. 2016.
- Arab crowdfunding. 2016. Arabcrowdfunding.com
- Arabnet Business Intelligence (ABI). 2016. Digital Bank Adoption in MENA 2016.
- Arabnet Business Intelligence (ABI). 2017. KSA Innovation Economy Tech Startups.
- Asia Development Bank (ADB). 2016. Digital Financial Services in the Pacific Experiences and Regulatory Issues. <https://www.adb.org/publications/digital-financial-services-pacific>
- Boston Consulting Group (BCG). 2016.
- Cambridge Center for Alternative Finance. 2017. The Africa and Middle East Alternative Finance Benchmarking Report. University of Cambridge. February 2017.
- Citigroup. 2017. Digital Disruption Revisited. What FinTech VC Investments Tell us About a Changing Industry. January 2017
- Chance Clifford. 2017. Fintech in the Middle East – An Overview.
- Crisanto, Juan Carlos and Prenio Jermy. 2017. Regulatory approaches to enhance banks' cybersecurity frameworks. Financial Stability Institutions (FSI) Insights on policy implementation No 2. August 2017
- DLA Piper. 2017. Data Protection Laws of the World
- Dubai Technology Entrepreneur Center (Dtec), Dubai Silicon Oasis Authority (DSOA), IBM. 2017. The Cloud Report. Navigating the Cloud as a Dubai Start Up.

- Price Waterhouse and Coopers (PWC). 2016. A false sense of security? Cybersecurity in the Middle East. www.pwc.com/me/cybersecurity.
- M.N. El-Guindy, Middle East Cyber Security Threat Report 2014, December 2013, http://www.academia.edu/5522905/Middle_East_Cyber_Security_Threat_Report_2014
- European Bank for Reconstruction and Development, the European Investment Bank, or The World Bank (EBRD, EIB and World Bank). 2016. What's Holding Back the Private Sector in MENA. Lessons from the Enterprise Survey.
- Federation of Egyptian Banks (FEB) and Federation of Egyptian Industries. 2017. Facilitating Bank Account Transactions: A Step Towards Financial Inclusion in Egypt. Policy Recommendations September 2017.
- Financial Stability Board (FSB). 2017. Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention. June 2017
- GSMA. 2016. GSMA Intelligence Global mobile trends October 2016
- IISS. 2013. Considerations for Regulatory and Policy Approaches to Cloud Computing in the GCC. IISS White Paper.
- International Comparison Legal Guides (ICLG). 2017.
- International Monetary Fund. 2017. Fintech and Financial Services: Initial Considerations. by Dong He, Ross Leckow, Vikram Haksar, Tommaso Mancini-Griffoli, Nigel Jenkinson, Mikari Kashima, Tanai Khiaonarong, Céline Rochon, and Hervé Tourpe
- International Monetary Fund (IMF). 2017b. Global Financial Stability Road. A Bumpy Road Ahead. April 18, 2018.
- International Monetary Fund (IMF). 2016. Virtual Currencies and Beyond: Initial Considerations. Staff Discussion Note SDN/16/03 by staff team comprising Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes
- Kaspersky Lab. 2017. Mobile Malware Evolution 2016
- Latham and Watkins. 2017.
- Lukonga, I, Naceur, S, Hadjian, G and Al-Hassan, A. 2014. Access to Finance for Small and Medium-Sized Enterprises in the MENAP and CCA Regions in Middle East and Central Asia, Regional Economic Outlook, October 2014.
- Lukonga, I. 2017. Fintech in the MENAP and CCA: Growth, Opportunities and Challenges in the MENAP and CCA Regions in Middle East and Central Asia, Regional Economic Outlook, October 2017.

- McKinsey & Company. 2016a. Digital Middle East: Transforming the region into a leading digital economy. October 2016.
- McKinsey & Company. 2016b. Digital Banking in the Gulf. Keeping pace with consumers in a fast-moving market place. Banking November 2016.
- Ministry of Trade and Economy (MOET). 2014. SME Guide Book. What is in Lebanon for SMEs. Republic of Lebanon.
- Ngatia, Isaac. 2017. State of Mobile Payments/Mobile Wallets in the GCC. Oct 2017 - Market Perspective - Doc # CEMA43127317
- Thompson Reuters. 2017. The Cloud Report. Navigating the Cloud as a Dubai Startup. Sponsored by Dubai Technology Entrepreneur Center (Dtec) Dubai Silicon Oasis Authority (DSOA) and IBM. 2017.
- Randstand. 2018. Top barriers to fintech growth in the Middle East. Randstandmena.com
- Sameh Aboul-Enein. 2017. Cybersecurity Challenges in the Middle East. GCSP. Geneva Papers. 22/17 Research Series
- Sidley. 2017. FinTech and Regulatory Sandboxes in the UK, Hong Kong and Singapore www.sidley.com/subscribe.
- Symantec. 2017. Internet Security Threat Report.
- Tanai Khiaonarong. 2014. Oversight Issues in Mobile Payments. IMF Working Paper WP/14/123
- Thales. 2018. Middle East Encryption Trends Study. Ponemon Institute. May 2018.
- Toronto Center. 2017. Fintech, RegTech and supTech: What they Mean for Financial Supervision. August 2017. TC Notes Practical Leadership and Technical Guidance from Toronto Center.
- Unipath. 2016. "The Fight against internet crime must not undermine good governance" in UNIPATH.
- World Economic Forum. 2015. The Global Information Technology Report 2015. ICTs for Inclusive Growth
- World Economic Forum. 2017. The Global Competitiveness Report 2017–2018
- World Bank. 2017a. Good Practices for Consumer Protection. 2017 Edition
- World Bank. 2017b. Global Financial Inclusion and Consumer Protection Survey 2017 Report
- World Bank 2017. Doing Business 2017: Equal Opportunity for All. Washington, DC: World Bank