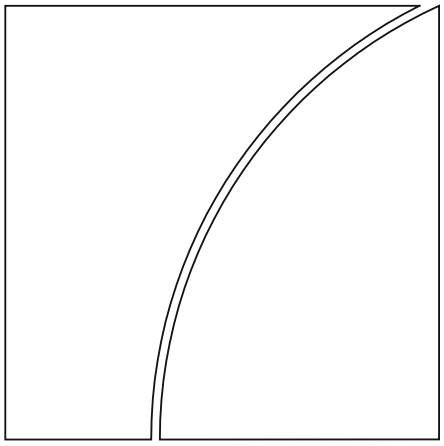
Committee on Payments and Market Infrastructures

World Bank Group



# Payment aspects of financial inclusion in the fintech era

April 2020

BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

This publication is available on the BIS website (www.bis.org).



ISBN 978-92-9259-345-2 (print)

ISBN 978-92-9259-346-9 (online)

# Table of contents

# Foreword

In 2016, the Committee on Payments and Market Infrastructures (CPMI) and the World Bank Group published the *Payment aspects of financial inclusion* (PAFI) report, which looked at financial inclusion from a payments perspective. The PAFI report envisaged that all individuals and businesses should have access to and use at least one transaction account operated by regulated payment service providers to: (i) perform most, if not all, of their payment needs; (ii) safely store some value; and (iii) serve as a gateway to other financial services.

New applications of technology to financial services, often referred to as "fintech", have accelerated in recent years. These developments have implications for how transaction accounts are provided, accessed and used as they underpin new products and services, such as instant payments, and enable new access modes, such as electronic wallets.

The CPMI and the World Bank Group have been analysing fintech developments in various contexts. For example, the CPMI has issued reports on digital currencies (November 2015), fast payments (November 2016), distributed ledger technologies in payments, clearing and settlement (February 2017) and, with the Markets Committee, central bank digital currencies (March 2018). The World Bank Group, together with the International Monetary Fund, published the Bali Fintech Agenda, which offers a framework for the consideration of high-level issues by individual member countries.

In October 2018, the CPMI-World Bank Group PAFI task force reconvened to deliberate on the experience gained from the implementation of the guiding principles and the accompanying key actions for consideration and the challenges ahead. In this last regard, the task force has produced this report to provide additional guidance on recent fintech developments that have relevant implications for PAFI's underlying objectives.

The CPMI and the World Bank Group are very grateful to the members of the task force, its co-chairmen Marc Hollanders (Bank for International Settlements) and Harish Natarajan (World Bank Group) and the co-leads of the fintech workstream, Maria Teresa Chimienti (European Central Bank) and Thomas Lammer (Bank for International Settlements and formerly European Central Bank).

Jon Cunliffe
Chair
Committee on Payments and Market Infrastructures

Ceyla Pazarbasioglu
Vice President
World Bank Group

# Executive summary

Financial inclusion starts with payments. They serve as a gateway to other financial services, such as savings, credit and insurance. Transaction accounts operated by a regulated payment service provider are at the heart of retail payment services. To improve financial inclusion, these transaction accounts need to enable end users to meet most, if not all, of their payment needs and to safely store some value. On these key premises, the Committee on Payments and Market Infrastructures and the World Bank in 2016 issued guidance on payment aspects of financial inclusion (PAFI) (CPMI-World Bank (2016)), as laid out in the first section of this report. The 2016 PAFI report outlines seven guiding principles for public and private sector stakeholders and contains possible key actions for countries that wish to put these guiding principles into practice. Since then, the PAFI framework has been adopted as the analytical underpinning for designing and implementing country-level actions and global efforts to improve access to and usage of safe transaction accounts.

Technological innovation has made major inroads into financial services, especially payments. The pace of innovation has substantially increased in the past five years, leading to the "era of fintech". This report defines fintech as advances in technology that have the potential to transform the provision of financial services, spurring the development of new business models, applications, processes and products. New technologies are at the core of fintech, which in turn has implications for payment product offerings and access modes. Section 2 of the report provides an overview of fintech developments that are relevant to the payment aspects of financial inclusion.

Fintech presents both opportunities and challenges in improving access to and usage of safe transaction accounts, as discussed in Section 3. Fintech can be leveraged to improve the design of transaction accounts and payment products, make them ubiquitously accessible, enhance user experience and awareness, and achieve efficiency gains and lower market entry barriers. At the same time, these benefits come with certain risks in terms of operational and cyber resilience, the protection of customer funds, data protection and privacy, digital exclusion and market concentration. If not adequately managed, these risks could undermine financial inclusion outcomes. This underscores the importance of effective regulatory, oversight and supervision frameworks. In addition, particular attention should be devoted to promoting responsible innovation that does not exclude disadvantaged segments of the population, by encouraging designs that are tailored to the needs of these segments.

Accordingly, as financial inclusion strategies seek to harness the benefits of fintech, it is equally important to address the attendant risks. Section 4 discusses the important roles of stakeholder commitment, the legal and regulatory framework, and financial and information and communication technology infrastructures to that extent. First, fintech developments call for increased international and cross-sectoral coordination, especially in the light of the cross-border and cross-currency nature of certain fintech innovations. Effective cooperation and coordination among central banks, financial supervisors, regulators and policymakers can help avoid potential regulatory arbitrage and promote effective oversight and supervision. Second, continued efforts by authorities to keep pace with innovation will help to avoid gaps in regulatory, supervisory and oversight frameworks, and to address challenges in their application to new business models. Finally, fintech developments have highlighted the opportunities and challenges of broadening payment service providers' access to payment infrastructures and the need to raise the bar for cyber resilience, and created momentum for cross-border interoperability.

The 2016 PAFI guidance for advancing financial inclusion through payments was formulated in a technology-neutral and holistic way, and continues to be relevant in the era of fintech. Stakeholders aiming to leverage the fintech potential in a responsible way for achieving the PAFI objectives can take further actions that seek to harness the potential of fintech, while mitigating its accompanying risks. Section 5 sets out these fintech-focused key actions, and places them in the context of the 2016 PAFI guidance. These key actions are based on the analysis carried out in this report and on country experiences. Both the fintech specific extensions and the original recommended key actions for consideration are not intended

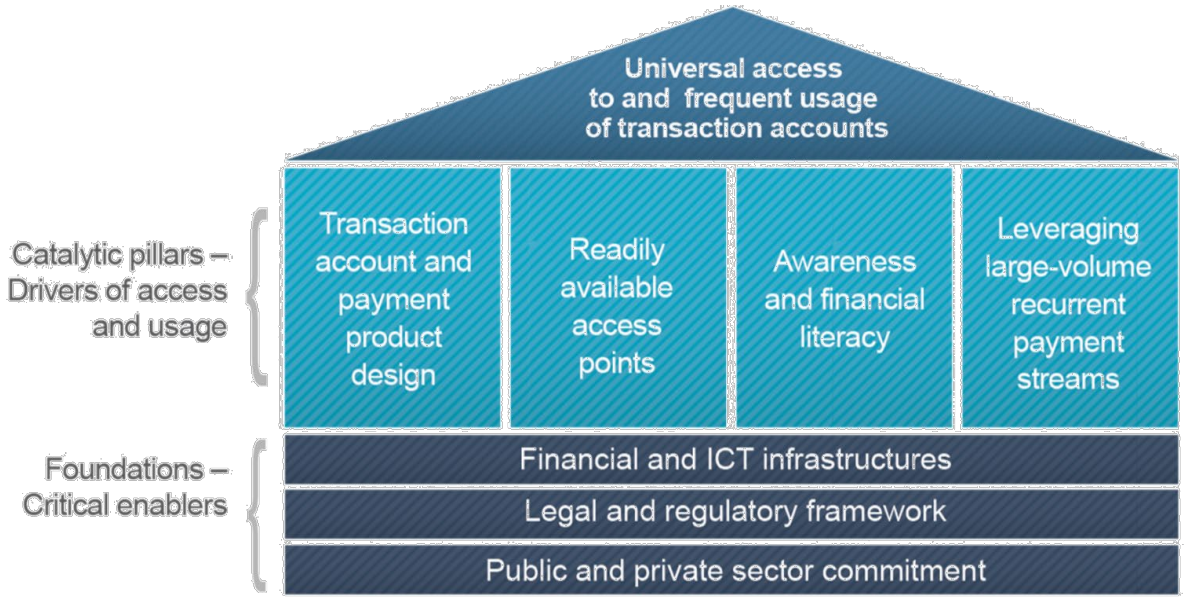
to provide a one-size-fits-all blueprint, as different country conditions may warrant different and customised approaches.

In conclusion, fintech can support improved access to safe transaction accounts and encourage their frequent use. However, it is not a panacea and there are risks that need to be managed. To realise fintech's potential to improve financial inclusion, initiatives need to be appropriately embedded in wider country-level reforms and global efforts that seek to put the PAFI guidance into practice.

# 1. Introduction

1. In 2016, the Committee on Payment and Settlement Systems (CPMI) and the World Bank published a report on payment aspects of financial inclusion (hereafter, PAFI report) that looked for the first time at financial inclusion from a payments perspective. The PAFI report envisages that all individuals and businesses have access to and use at least one transaction account[1] operated by a regulated payment service provider (i) to perform most, if not all, of their payment needs; (ii) to safely store some value; and (iii) to serve as a gateway to other financial services. However, a number of barriers affect transaction account access and usage. To address those barriers, the PAFI report outlines a framework (the "PAFI house", Figure 1) comprising foundations, ie the critical enablers for payment systems and the provision of payment services, and catalytic pillars, ie the drivers of access and usage. Both foundations and pillars contribute to the end objective of achieving universal access to and usage of transaction accounts. The PAFI report analyses each component of this framework and provides suggestions in the form of guiding principles and key actions for consideration.[2] The PAFI framework has since been used as a basis for the design and implementation of global initiatives, country-level reforms and developing surveys and measurement tools to track progress on access to and usage of transaction accounts.

Framework for the guidance on payment aspects of financial inclusion — Figure 1




Source: CPMI-World Bank (2016).

2. More recently, institutions and organisations with an interest in financial inclusion have emphasised the potential of fintech for increasing financial inclusion, while recognising that it also comes with new challenges. The International Monetary Fund (IMF) and the World Bank have acknowledged the

[1] A transaction account is broadly defined as an account held with a bank or other authorised and/or regulated service provider (including a non-bank) which can be used to make and receive payments. Transaction accounts can be further differentiated into deposit transaction accounts and e-money accounts.

[2] The PAFI guiding principles and key actions for consideration can be found in Section 4 of the 2016 PAFI report and they are listed together with key actions for consideration focusing on fintech in Section 5 of this report.

potential of fintech to support the Sustainable Development Goals (SDGs) in general and financial inclusion specifically. The Bali Fintech Agenda, adopted in 2018, features 12 elements that look at fintech issues in a holistic way, many of which focus specifically on financial inclusion and on elements of relevance to this report.

3. In October 2018, the CPMI and the World Bank reconvened the Task Force on Payment Aspects of Financial Inclusion to (i) produce tools to facilitate the application of the PAFI guidance; (ii) develop a measurement framework and other tools to assist countries in tracking their progress on improving access to and usage of transaction accounts; and (iii) provide additional guidance on recent fintech developments that have relevant implications for PAFI's underlying objectives. This report is a response to that last item.

4. Advances in technology can have a positive impact on access to cross-border payments. Enhancing cross-border payments is the first priority in the Saudi Arabian G20 Presidency's financial regulation agenda. The Financial Stability Board (FSB) and CPMI are working together to assess the current challenges in cross-border payments, create a response with a list of actions to improve them and develop a roadmap by October 2020. The work will take into account the conclusions of this report to ensure that the roadmap harnesses the possibilities of technological innovation for enhancing cross-border payments and does not introduce obstacles to future innovation.

5. This report defines fintech as *advances in technology that have the potential to transform the provision of financial services, spurring the development of new business models, applications, processes and products* (IMF-World Bank (2018)). Fintech activities can be observed in different types of financial services, such as deposits, lending and capital raising, insurance, investment management, and payments, clearing and settlement (FSB (2017)). The scope of the present report is limited to fintech in the context of payments, clearing and settlement, to the extent that they can be leveraged to increase access to and usage of transaction accounts, ultimately improving financial inclusion.

6. While fintech is a relatively new concept, innovation has been shaping the evolution of payment services over time and has served as a driver of payment system reform. The PAFI report acknowledges the role of innovation (eg electronic money, especially mobile money) in facilitating access to and usage of transaction accounts. It also emphasises the importance of enhancing existing infrastructures and adopting new delivery models to broaden the reach of traditional payment instruments and products. The report provides guidance on designing a legal and regulatory framework that fosters innovation without compromising the safety and integrity of the financial system. At the same time, the PAFI report maintains a neutral stance towards the technology used, thereby ensuring broad applicability of the PAFI guidance. This stance remains valid today, the era of fintech. Nevertheless, the increasing momentum gained by fintech developments may alter the payments landscape along with the prospects for financial inclusion.

7. It is therefore important and timely to identify the promise fintech holds for financial inclusion and how to responsibly harness that potential. This report (i) reviews fintech developments with a focus on payments; (ii) analyses how they can help remove the obstacles to universal access to and frequent usage of transaction accounts, including by providing examples of concrete initiatives; and (iii) provides additional guidance focused on fintech under the PAFI guiding principles. This report is the first of three deliverables of the reconvened PAFI Task Force. It will be complemented by a toolkit on the implementation of the PAFI guidance and a measurement framework.

8. This report is organised into five sections. Section 2 provides an overview of fintech developments relevant to the payment aspects of financial inclusion. Section 3 analyses the potential of fintech to increase access to and use of transaction accounts, on the one hand, and the associated challenges and risks, on the other. Section 4 discusses the characteristics of the critical enablers that allow the potential of fintech to be harnessed to achieve the PAFI objectives while addressing its risks. Section 5 draws the relevant conclusions for the PAFI guidance and puts forward additional fintech-specific considerations.

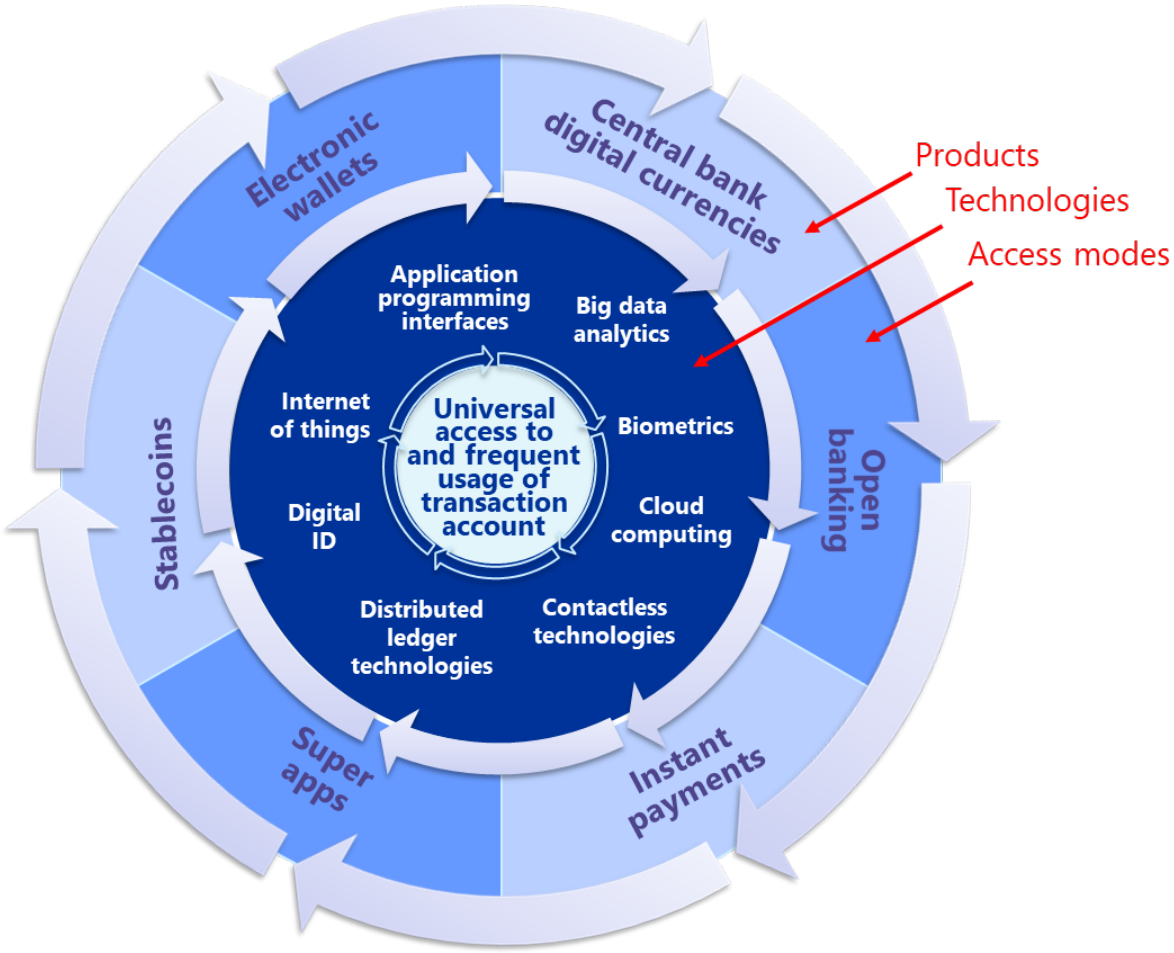
## 2. Fintech developments of relevance to the payment aspects of financial inclusion

9. This section provides an overview of selected advances in technology considered to be relevant to payments and describes their application to new payment products and services as well as new access channels. Application programming interfaces (APIs), big data analytics, biometric technologies, cloud computing, contactless technologies (including quick response (QR) codes), digital identification, distributed ledger technologies and the internet of things have been identified in this report as the most relevant new technologies in this context. They facilitate the delivery of new products and access modes. Prominent examples of new products are instant payments, central bank digital currencies (CBDCs) and stablecoins. New technologies not only offer new modes of accessing these new products by means of electronic wallets, open banking and super apps, but also allow payments to be initiated via traditional transaction accounts and/or payment instruments.

10. It is worth noting that new technologies can also be applied to existing products and/or access channels in a variety of combinations (eg initiation of card payments via electronic wallets leveraging contactless technologies). On the other hand, new products and access modes do not necessarily rely on advances in technology, but can simply use existing technologies in an optimised way (eg instant payments can be offered based on traditional technologies and initiated via online banking rather than electronic wallets).

11. The "PAFI fintech wheel" (Figure 2) directs focus onto new technologies in the centre. These new technologies are not indispensable for the product and access layer, but are in many cases harnessed to improve the provision of these new products and access modes.

Fintech developments potentially relevant to the payment aspects of financial inclusion: the "PAFI fintech wheel" Figure 2




## 2.1 New technologies

### 2.1.1 Application programming interfaces

12. Application programming interfaces (APIs) prescribe the way software programmes communicate and interface with each other (FSB (2019a)). APIs can be kept private or made publicly available (open or public APIs) to allow developers to integrate certain functionalities into their applications. They can be proprietary, with service providers designing different API interfaces and protocols, or standardised across service providers. The concept of APIs is not new, dating back as it does to the late 1960s. What is new is their increased application to financial services in general and payments specifically. Following legal and regulatory changes in several jurisdictions, the number of APIs that have been registered for the purpose of financial services and payments has increased sharply since 2016 (Santoro et al (2019)).

13. In payment and financial services, APIs underpin payment initiation services and broader open banking models (Section 2.3.2). APIs can also be used in electronic know-your-customer (e-KYC) [3] processes and to support checks on anti-money laundering/countering the financing of terrorism (AML/CFT), by enabling selected data to be shared among financial institutions while ensuring the privacy of data not needed for customer due diligence (CDD) purposes. Finally, APIs are being used by payment service providers (PSPs) to facilitate integration with merchants, particularly in the e-commerce space, and to interface with payment systems

14. There are several standardisation initiatives under way, eg to develop common functional and technical API specifications addressing the requirements of the Revised Payment Services Directive (PSD2) and associated regulatory technical standards (EBA (2018)).

### 2.1.2 Big data analytics

15. Big data is a generic term that designates the massive volume of data that is generated by the increasing use of digital tools and information systems (FSB (2017)). Big data analytics can be described as technologies that enable analysis of the significantly increased volume, variety, velocity and validity of data. Nowadays, the magnitude of data is substantially larger than can be accommodated by common spreadsheet applications. Big data analytics therefore uses a variety of tools, including artificial intelligence (AI), machine learning (ML) and deep learning (DL).[4] The success of big data analytics has been enabled by a confluence of different factors and new technologies, such as increased processing power and lower costs of data storage (thanks eg to cloud computing), as well as a greater availability of increasingly granular data (eg generated by the internet of things (IoT)) that can be transferred without human intervention via APIs and validated automatically on a consensus basis via distributed ledger technology (DLT) (FSB (2017), di Castri et al (2019)).

16. Big data analytics has made inroads into payment and financial services and is expected to become an essential business driver across the financial services industry in the short run. New providers are augmenting financial data with other data sets. In order to gain a better understanding of the end user, they are proactively collecting data through increased customer interaction and tracking customer behaviour on their platforms, eg mobile telephony, social media, and psychometric and geospatial data (Schiff and McCaffrey (2017)). On the other hand, banks have faced constraints in their ability to analyse customers' financial data across different business areas within the same institution, let alone in augmenting the information with external data (Zunzunegui (2018)). However, this is changing: increasingly, banks and other PSPs are adopting big data analytics. In Europe, 64% of financial institutions have launched big data analytics and only 2% do not have any related activity at all, while the remainder are in the discussion, development or piloting stage (Zunzunegui (2018), EBA (2020)). Current implementations, especially among traditional providers, are mainly focusing on risk management, followed by the generation of new revenue potential through new products and processes enabled by big data analytics (CCAF-WEF (2020)).

17. Big data analytics can support the onboarding of new customers through screening processes (eg by providing information required for KYC, checking different spellings of a name against sanction lists, and making predictions about a person's creditworthiness). Big data can thereby help improve the

[3] E-KYC refers to electronic means to conduct the customer's identification process and allows the digital or online verification of customer identity.

[4] AI allows computer systems to perform tasks that have traditionally required human intelligence. ML allows computers to learn with limited or no human intervention, by designing a sequence of actions (algorithms) to solve a problem that are updated automatically through experience. DL is a field of ML that uses multiple layers of learning algorithms to extract meaning from large quantities of data.

precision of real-time approvals and reduce the number of false rejections. For the purpose of authenticating and authorising existing customers, big data analytics can leverage a variety of granular data (eg a person's biometric features, combined with geographical and behavioural information). Throughout the transaction process, big data analytics is leveraged for risk mitigation and to detect and prevent fraud and other malicious activities. Furthermore, natural language processing[5] can help provide a personalised, conversational, and natural experience via chatbots and robo-advisers that can give advice, address customer complaints or improve self-service interfaces (FSB (2017), EBA (2020)).

### 2.1.3 Biometric technologies

18. Biometric technologies use an individual's unique physiological and behavioural attributes to establish and authenticate his or her identity. Physiological attributes include elements related to the shape and features of a body, such as fingerprints, iris or vascular patterns, and facial characteristics. Examples of behavioural attributes are gait, handwritten signature, keystroke patterns, and touchscreen and mouse usage. The usage of biometrics can complement, and even in some cases replace, traditional means of proving an end user's identity and thereby preventing and/or detecting fraud.

19. Biometric data are considered to be highly sensitive, and the highest security standards are essential when processing and/or storing them. Two different approaches to executing biometric matching are currently being pursued, ie within a centralised server environment or locally on the end user's device. While proponents of the centralised server approach argue that strict security standards can be more easily enforced and monitored, advocates of on-device matching (such as Apple or the FIDO Alliance) argue that their approach eliminates the risk of a large-scale data breach (Leong et al (2018)). Irrespective of the architectural approach, it is important to ensure the integrity of the process through which biometric data are linked to the individual. Further, irrespective of the architectural approach, biometric verification and/or authentication might rely on the end user's device (with an increasing number of smartphones offering fingerprint or facial identification features) or a device provided by the PSP (eg point of sale (POS) terminals or automated teller machines (ATMs) with biometric sensors).

20. In payment and other financial services, biometrics can overcome some of the challenges associated with personal identification numbers (PINs), passwords or social security numbers, among others. Innumerate and/or illiterate end users can be offered a better user experience, facilitating adoption of financial services. Depending on the use case, different biometric features, or a combination thereof, might be applied. Biometric characteristics can also be among the proof-of-identity requirements for the registration and activation of SIM cards to access mobile services (and, by extension, mobile financial services) (GSMA (2019a)). Biometric technologies can be leveraged for remote onboarding of customers, by traditional PSPs as well as new entrants, eg by matching images in an ID document with an image or a video of potential new customer. A quarter of BBVA's Spanish customers and 38% of its US customers, for example, used online or mobile channels to open an account as of the first quarter of 2019 (BBVA (2019); see also Section 2.1.6 on digital identification).

### 2.1.4 Cloud computing

21. Cloud computing enables the use of an online network ("cloud") of hosting processors to increase the scale and flexibility of computing capacity (FSB (2019)). Cloud computing thus enables ubiquitous, on-demand network access to shared configurable computing resources, including networks, servers, storage, applications and services, that can be rapidly provided and released via the cloud (Mell and Grance (2011)).

[5] Natural language processing is an interdisciplinary field of computer science, AI and computation linguistics that focuses on programming computers and algorithms to parse, process and understand human language (FSB (2017)).

22. Cloud computing is the main enabling technology for banking as a service (BaaS) – and, more specifically, payment as a service (PaaS) – delivery models. While cloud computing can be leveraged by PSPs to migrate existing software or payment processes to the cloud, PaaS platforms typically have a modular service offering, giving flexibility to PSPs to choose the services they need at any given time. BaaS and PaaS providers can be technology service providers[6] (eg ACI Worldwide or Margeta) or financial institutions (eg JPMorgan Chase and ClearBank) (McKinsey (2019)).

23. Cloud computing and delivery models such as BaaS and PaaS can serve as a tool to "democratise" access to technology by PSPs of all sizes and as an enabler of innovation in payments and associated services. In particular, it reduces the need for large investments in IT, thereby lowering market entry barriers for new providers. Meanwhile, it also makes it easier for traditional providers to implement newer, more competitive customer interfaces in a flexible manner. Since providers are required to pay only for the services they use, cloud computing is often a more cost-effective solution compared with the ongoing costs of proprietary IT infrastructure.

24. Cloud computing may also provide financial institutions with features and services that promote greater security and have higher degrees of operational resilience when compared with traditional practices. For instance, financial institutions can opt to build a private cloud, move across clouds or use multiple cloud service providers for a variety of cloud-based services. Such approaches can help avoid vendor capture and result in the provision of more affordable cloud services for many financial firms, but can also increase security and resilience.

25. Some jurisdictions have introduced data localisation requirements for sovereignty reasons or in view of concerns that cloud services might reduce authorities' ability to access data or inspect the cloud provider's facilities. Furthermore, many countries have either modified their existing regulatory frameworks or clarified their regulatory expectations on the use of cloud computing by financial institutions with the intention of ensuring that financial institutions adequately manage the risks associated with the use of cloud computing (Dias and Izaguirre (2019), Ehrentraud et al (2020)).

### 2.1.5 Contactless technologies

26. Contactless technologies facilitate the acceptance of payment instruments at the point of sale. The key characteristic of contactless technologies is the transmission of payment information from a physical device without the need for physical contact between the payee's acceptance device and the payer's payment instrument. Information used for contactless payments can be stored on and/or accessed via a variety of physical devices (eg payment cards, mobile phones, wearables).

27. When an end user initiates a payment transaction at the point of sale via contactless technologies, the user's device communicates with the POS terminal eg via radio frequency identification (RFID)[7] or near field communication (NFC).[8] However, the concept of "contactless" extends beyond that of RFID and NFC

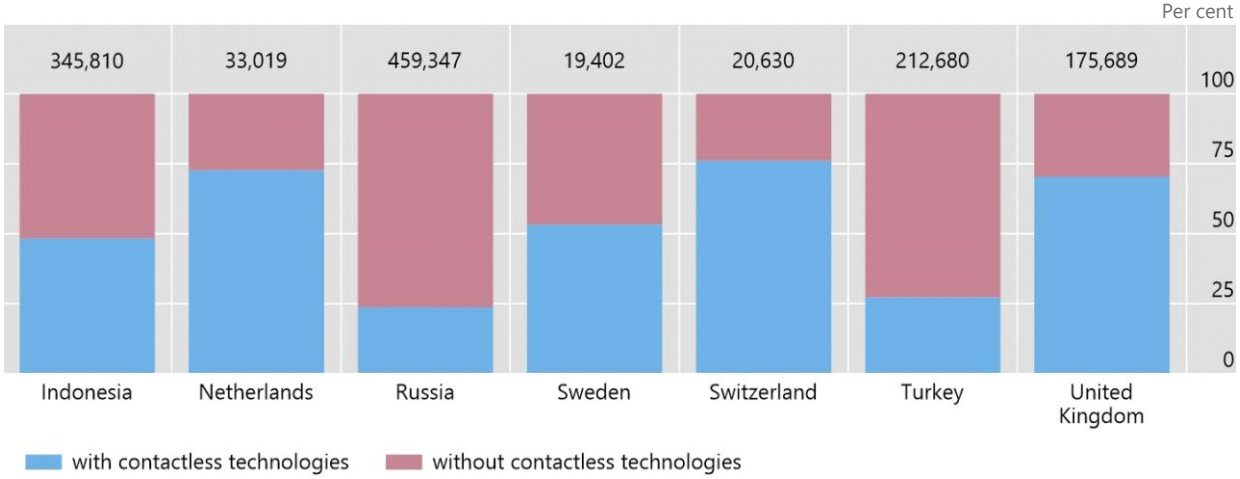
[6] Sometimes BaaS is defined as a combination of banking tech stack and banking license, while those services offered by technology service providers being qualified as Software-as-a-Service (Jenik and Zetterli (2020)).

[7] RFID is a technology that allows objects to be "tagged" with an identifier that can be read remotely using either inductive electromagnetism or emitted radio waves. Due to the very broad range of applications, the distances at which tags may be interrogated vary considerably (from a few centimetres up to 10 metres) according to the operational requirements (ETSI (2011)).

[8] NFC is a standards-based, short-range (a few centimetres) wireless connectivity technology that enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content and connect electronic devices with a single touch (NFC Forum (2013)).

and also includes other technologies, eg Bluetooth low-energy (BLE)[9] and QR[10] codes. The number of payment cards issued with contactless technologies has increased considerably in some jurisdictions. In the Netherlands, Sweden, Switzerland and the United Kingdom, the majority of cards issued already feature contactless technologies (Graph 1). In Denmark, 72% of all card payments at the point of interaction were made contactless in the third quarter of 2019 (Danmarks Nationalbank (2019)).

Share of cards with contactless technologies in selected countries[1] Graph 1




[1] Data for 2018. Figures in thousands represent the total number of cards issued in the respective country.

Source: CPMI (2019b).

28. Contactless technologies, in combination with tokenisation, are instrumental to the provision of electronic wallets (Section 2.3.1). Tokenisation is the process whereby sensitive data are replaced with a surrogate value, known as a token, in order not to expose the original data. More specifically, tokens used in payments are a disguised representation of underlying sensitive payment data (ie data that can be leveraged to carry out fraud), such as transaction account or payment card numbers, with the ultimate objective of protecting the underlying accounts (Box A). The use of tokens does not alter the normal course of payment processing, apart from the tokenisation and de-tokenisation processes. Tokenisation can be implemented as a proprietary solution or based on international standards.

[9] BLE is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications, including beacons. Compared with classic Bluetooth, BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range. As retailers continue to drive payments innovation, BLE is likely to have a significant role to play (Stoorvogel (2019), EPC (2019)).

[10] The QR code is the trademark of a type of matrix barcode created in the 1990s, and is being used by many industries and in different contexts. While similar to linear barcodes, QR codes can store a larger volume of data; can be scanned not only from paper but also from screens; can be used even if partially damaged; and can encrypt information. QR codes can be scanned with a barcode reader or the camera of a mobile device (Sorensen (2019)).

Box A

## Tokenisation in payments

Tokenisation is part of a broad industry effort to protect sensitive payment data where they are more vulnerable, ie while stored or in transit across the merchant environment. Tokenisation has become a cornerstone for enabling card digitalisation, helping to secure a new generation of digital solutions for mobile payments and e-commerce.

Payment tokenisation is a security technology that supports innovation while mitigating fraud and data security risks, in combination with encryption and cryptography. Tokenisation is a security measure where the actual card details (ie expiry date and primary account number (PAN)) are replaced with unique digital identifiers (tokens) which can be parametrised for restricted use. For example, a token provisioned to a mobile phone could be set up to initiate only proximity payments, from that particular device, by a given cardholder. A token could be issued for in-app payments at a specific merchant only. Additionally, a token might be set to be valid for a single use, or restricted to a number of purchases before expiring.

The security strategy consists in devaluing tokens as payment credentials, making them less sensitive and less exploitable than traditional PANs. Prior to authorising a tokenised transaction, the issuer, or the designated token service provider (TSP) on its behalf, is responsible for decrypting the payment token and applying the aforementioned restriction controls, to ensure that a genuine token is used within one of the acceptable domains for that given token, thereby limiting the potential uses of a compromised token. As a result, tokenised payment credentials become less attractive to fraudsters, and tokenisation helps reduce the costs associated with data breaches.

While tokenisation was not originally conceived as an authentication solution, it has become useful in the context of the strong customer authentication (SCA) requirements of PSD2. Potentially, a token-based payment instrument could contribute to providing evidence of possession, if the proper security measures are implemented. In fact, security and usability benefit enormously from binding both token and payer to a trusted device with authentication capabilities, such as biometrics. Enriched data stemming from the token assurance and the consumer device used to initiate payment transactions are useful risk assessment factors for PSPs to effectively reduce online fraud.

The Reserve Bank of India granted card networks permission to offer card tokenisation services for a specific use case in 2017. In 2019, general permission was extended, enabling all authorised card networks to offer tokenisation services to all use cases/channels (eg NFC/magnetic secure transmission (MST)-based contactless transactions, in-app payments, QR code-based payments) or token storage mechanisms (cloud, secure element, trusted execution environment, etc). Tokenisation and de-tokenisation can be performed only by an authorised card network, and the original PAN may be recoverable only by that network. A token requester may not store a PAN or any other card detail. The existing instructions make no concessions for the additional factor of authentication (AFA). Registering for tokenisation has been made purely voluntary for customers, who are not charged for availing themselves of this service. Customers have the option of registering/de-registering their card for a particular use case, eg contactless, QR code-based, in-app payments. Customers also have the option of setting and modifying per-transaction and daily transaction limits for tokenised card transactions. For the present, this facility is being offered through mobile phones/tablets only. Its extension to other devices will be examined based on the experience gained.

Sources: ECB; Reserve Bank of India.

### 2.1.6 Digital identification

29. Digital identity, or digital ID, refers to a set of electronically captured and stored attributes and credentials that can uniquely identify an individual or legal person and is used for electronic transactions (Mittal (2018)). A person's digital identity may be composed of a variety of attributes, including biographic data (eg name, age, gender, address) and biometric data (eg fingerprints, iris scans, hand prints) as well as other attributes that are more broadly related to what the person does or something someone else knows about the individual (Natarajan et al (2018)).

30. An estimated 1 billion people worldwide do not have basic identification credentials, and many more have IDs that cannot be trusted because they are of poor quality or cannot be reliably verified. Most

of the affected individuals live in Sub-Saharan Africa and South Asia. According to the World Bank Group's 2018 ID4D Global Dataset, 63% of those without basic identification credentials live in lower-middle-income economies, while 28% live in low-income economies. Women are more likely than men not to have a proof of identity, especially in low-income economies, where 30% of men and 45% of women lack foundational ID (ie they are not captured by civil registries, national IDs, universal resident ID systems or population registers). According to the 2017 Global Findex Survey, the lack of documentation was also a significant barrier to accessing financial services cited by 20% of adults without an account. One estimate is that 3.4 billion people have some form of ID but have limited ability to use it in the digital world. In this context, the introduction of digital IDs could provide universal coverage while potentially increasing the adoption of transaction accounts and financial services, eg by enabling remote customer onboarding (Demirgüç-Kunt et al (2018)).

31. Micro-, small and medium-sized enterprises (MSMEs) without formal business registration documentation can face similar problems in gaining access to financial services if they cannot establish the identities of the staff and directors authorised to set up, operate and instruct changes for the business. Some countries have taken action to address this problem. Canada, for example, has introduced a number with which to identify businesses at the national level, and Serbia has a unique digital ID for all business people as a form of identification within the country. Aadhaar in India is being used to assert, among other things, the ownership of businesses (through the Udyog Aadhaar registration process for MSMEs, where an Aadhaar number is associated with a company registration) (Natarajan et al (2018)). For SMEs, the adoption of the Legal Entity Identifier (LEI) in the non-financial corporate sector could increase the value of their data by enabling the identification of their businesses and verification of their data. Such high-quality data can increase their access to and choice from a range of financial services (Cleland and Hartsink (2020)).[11]

32. In the absence of, or lack of access to, government-issued identification documents, alternative data can be used to support the proof of identity. Low-income communities might not have any street names as such, or any street names that do exist might not be recorded in land registries. In India, for example, residents of such communities are starting to use smartphone location data to locate themselves on city maps and to register for an address that they can then use to receive mail and apply for government IDs. Furthermore, if traditional records have been destroyed (eg in the event of conflict or natural disasters), mobile phone records can feed into a proof of record (WEF (2019)). For end users that already have access to a transaction account, transaction account data themselves can enable them to access other (financial) services and/or serve as a proof of identity (Section 3.1.2).

Box B

## Digital ID infrastructures can help realise the opportunity to digitalise government payments

The PAFI report identifies the potential of government payment programmes, especially benefit programmes, to directly advance financial inclusion by providing transaction accounts to the recipients and strengthen the enabling environment for payment services. The World Bank estimates that digitalising government-to-person (G2P) payments would result in 167 million adults gaining access to a transaction account.

[11] The LEI is a 20-character alphanumeric code, designed to uniquely identify any legally distinct entity that engages in financial transactions. Its aim is to provide a globally consistent and unique code for each legal entity; separate from any domestic registration (Cleland and Hartsink (2020)).

A legal, unique and digital ID is a critical element in delivering government services with greater efficiency, particularly G2P payments, and in addressing financial access and broader inclusion for individuals and MSMEs. Digital IDs offer the potential for countries to rapidly advance their identification goals and improve the quality and utility of ID systems. For example, digitalised databases of records, compared with physical ledgers stored in a local office, make it easier to verify a person's records remotely, creating efficiencies for service delivery and allowing ID agencies to replace credentials and records that have been lost, stolen or destroyed. Digital authentication mechanisms facilitate automated transactions that are more secure and reliable than manual authentication (ie visually comparing a person presenting an ID against their photo) and can reduce the amount of personal information revealed in a transaction (eg attribute-based credentials). The use of automated biometric recognition (eg fingerprints or iris scans) can help ensure that identities are unique (ie that people cannot enrol multiple times) and provide a convenient, password-free method of authentication.

However, digital ID infrastructures bear many of the risks associated with collecting and managing personal data digitally. When databases are digitalised, the risk and scale of breaches and identity theft are also elevated. In addition to potential privacy violations, the digitalisation of identification can also create new barriers to access and inclusion. Certain populations, such as manual labourers with worn fingerprints, the elderly or individuals with disabilities, may have difficulty enrolling in or using ID systems that rely on certain types of biometrics, which can lead to exclusion if no alternative options are in place. Similarly, digital ID systems that rely on technologies that are not consistently or universally available among the population (eg internet connections, email, mobile phones) can also exacerbate the digital divide.

Sources: World Bank (2016b, 2019b); Natarajan et al (2018); White et al (2019).

### 2.1.7 Distributed ledger technology

33. Distributed ledger technology (DLT) encompasses the processes and related technologies that enable nodes in a network (or arrangement) to propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes. In the context of payment, clearing and settlement, DLT enables entities, through the use of established procedures and protocols, to carry out transactions without necessarily relying on a central authority to maintain a single "golden copy" of the ledger (CPMI (2017)).

34. The emergence of DLT has been met with expectations that application of such technologies to the financial sector could help address, or ease, some of the long-standing challenges to enhancing access to financial services. These expectations originate from certain features of DLT, particularly automation and programmability, which can be associated with efficiency gains (eg greater transaction speed), cost reductions, and enhanced reliability and resilience, as well as new business opportunities. Under certain circumstances, DLT would therefore lend itself to applications that could prove beneficial to the underserved and unserved segments. These include applications for payments and settlements, identity management systems, and asset registries (eg land registry) (Natarajan et al (2017)).

### 2.1.8 Internet of things

35. The internet of things (IoT) encompasses software, sensors and network connectivity embedded in physical devices, buildings and other items that enable those objects to (i) collect and exchange data and (ii) send, receive and execute commands (FSB (2019a)). IoT goes hand in hand with big data (capturing the information) and analytics (understanding the information) by making information readily available and consumable by other systems and networks. IoT acts as an intermediary tool that helps utilise information for increased efficiency and productivity and improved user experience (Morgan (2014), WEF (2015, 2016)).

36. Payment and financial service providers are increasingly turning to IoT in combination with other innovative technologies to improve the customer experience and gain market share. However, harnessing the potential of IoT at scale depends on progress as regards a country's overall telecommunications

network infrastructure, big data analytics and cloud computing (WEF (2015)). Increased bandwidth may enable further innovation in payment and financial services. Yet, as the first countries launch 5G networks, as of 2018 about 60% of the population in low- and middle-income countries did not have any mobile internet connectivity at all (Bahia and Suardi (2019)).

37. IoT enables the integration of automated electronic payments into contractual arrangements while reducing the default risk for providers. One example is the pay-as-you-go (PAYG) model, eg the leasing of solar panels, whereby an initial deposit is made, followed by small instalments at regular intervals until the full value of the system is paid, as offered by M-KOPA in East Africa. Another example is interlinking smart meters for water or energy supply with payment solutions (often based on mobile money), which eliminates the need for end users to prepay their consumption on a monthly, quarterly or even annual basis, and instead allows them to pay for their actual usage in real time (WEF (2019)).

## 2.2 New products and services

### 2.2.1 Instant payments

38. For the purpose of this report, the term "instant payments" should be understood to mean payments in which the transmission of the payment message and the availability of final funds to the payee occur in seconds around the clock, 365 days a year.[12] An increasing number of retail payment systems around the world are meeting these criteria (Box C). Such systems are for the most part based on credit transfers, but there are also alternative implementation designs that rely on card payments or e-money. Instant payments may be central bank-driven (eg in Brazil and Mexico), industry-driven (eg in the United Kingdom) or the result of a joint approach (eg in Australia, where the central bank has subscribed as a participant to the development of the New Payments Platform). In Europe, the scheme governing instant payments was developed by the European Payments Council (EPC), whose members are banks and other PSPs, in dialogue with the regulators and other stakeholders. Based on the scheme, privately operated payment infrastructures as well as the Eurosystem have introduced clearing and/or settlement services for instant payments.

39. Instant payments resemble features of cash in a sense that funds are made available immediately to the payee and they can be used for person-to-person transfer. The fact that they can also be used for remote payments makes them an attractive option too for large-volume use cases such as government payments and recurrent payment streams such as remittances (for the time being, mostly domestic remittances). At the time of writing, instant payments have experienced significant uptake by the end user in several countries and have the potential to substitute for a relevant share of cash payments, traditional card payments and standard electronic funds transfers. In India, the transactions of Unified Payments Interface (UPI) reached 1 billion transactions per month in October 2019, substantially exceeding RuPay card payments, India's domestic card scheme (NPCI (2019)). Similarly, the Singaporean FAST payment scheme has almost caught up with card payments in terms of the value of transactions (85%) (MAS (2018)).

[12] As compared with the more general definition of "fast payments" (CPMI (2016)), or other terms commonly used in this space (eg faster payments, immediate payments), this report focuses on both the instant crediting of funds to the payee's account (ie within seconds) and the 24/7/365 availability, for which reason the term "instant payments" has been chosen.

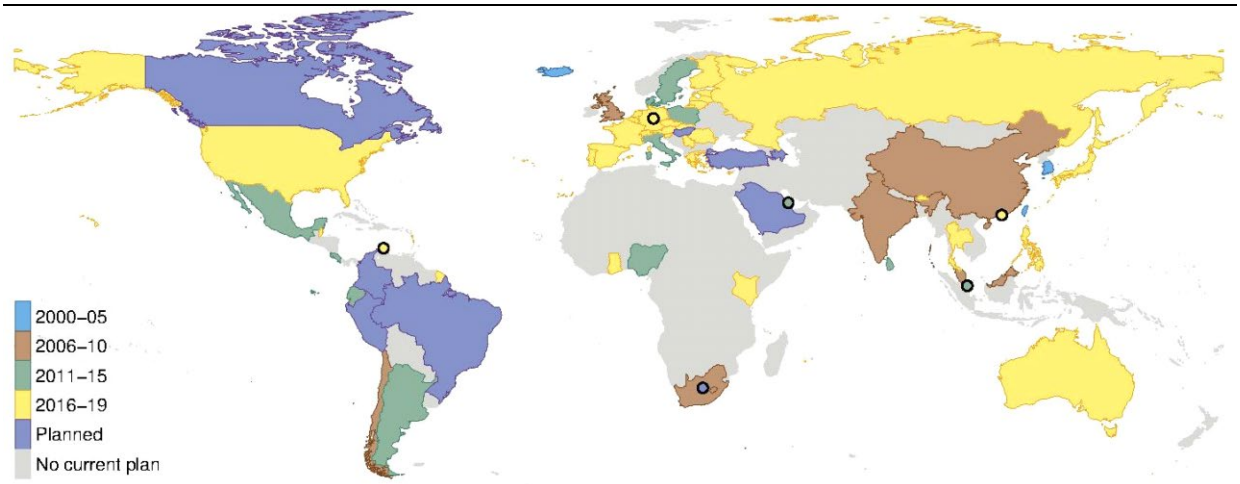
Box C

## Fast retail payment systems

*Fast (retail) payment systems* (FPSs) have been (or are being) developed in many jurisdictions. The CPMI defines a FPS is a system in which the transmission of the payment message and the availability of the final funds to the payee occur in real time or near real time on as near to a 24/7 basis as possible.① While closed-loop systems can also be near real time and available 24/7, FPSs are payment infrastructure that facilitates payments between account holders at multiple PSPs rather than just between the customers of the same PSP. Currently, 56 jurisdictions have FPSs, and this number is projected to rise to 64 in the near future (Figure C). While the adoption speed is fairly similar to that of wholesale real-time gross settlement (RTGS) systems, early adopters are predominantly emerging market rather than advanced economies.

### Geographical diffusion of fast payment systems

Figure C




The boundaries shown and the designations used on this map do not imply official endorsement or acceptance by the BIS.

The yellow circle in Europe represents the Eurosystem FPS. The FPSs in Aruba, Bahrain, Hong Kong SAR and Singapore are also represented by circles.

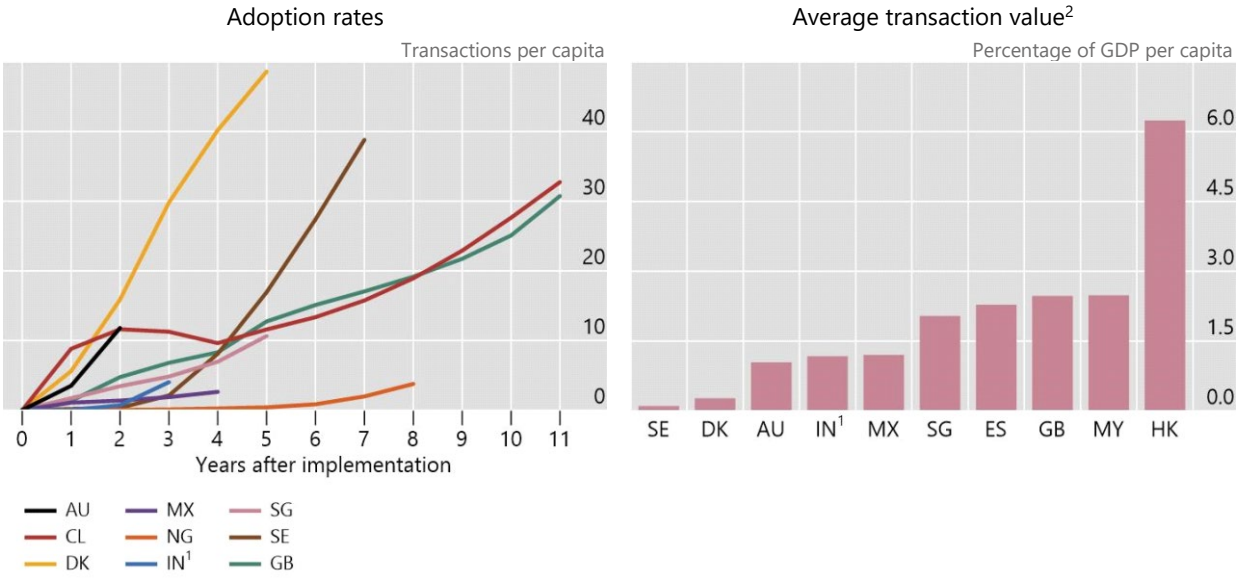
Sources: CPMI survey; national data.

Take-up and usage vary significantly across jurisdictions (Graph C, left-hand panel). The FPSs in Chile and the United Kingdom, which have been operating for 10 years, processed just over 30 payments per capita in 2018. In contrast, the FPSs in Sweden and Denmark were launched more recently but processed more payments per capita – 40 and 48, respectively – in 2018, respectively. This is largely due to the popularity and strong growth in the use of mobile payment apps that are the front end of the FPS in these jurisdictions. In Australia, growth in transaction volumes has also been very rapid, reaching an annualised rate of around 12 fast payments per capita per year in just the second year of operation.

The average transaction value of faster payments varies significantly, suggesting that FPSs are used for a variety of retail payments (Graph C, right-hand panel). The average transaction value of fast payments in Denmark and Sweden is less than 0.3% per capita, indicating they are mainly used for person-to-person payments. At the other end of the scale, the average transaction value of fast payments in the Hong Kong SAR is over 6%, suggesting that they are mainly used for payments involving businesses (eg payment of rent). In particular, the Hong Kong Monetary Authority's FPS enables real-time funds transfers in multiple currencies (the Hong Kong dollar and the renminbi) among deposit transaction accounts and non-bank electronic wallets. The mobile phone number or email addresses can be used as a proxy for account identification. These features attracted more than 3.6 million registrations (over 50% of total population) in Hong Kong SAR in the first 14 months after the system was launched in September 2018.

## Fast retail payment systems

Graph C




[1] Indian figures comprise only fast payments via Unified Payments Interface (UPI). [2] Data for 2018.

Source: CPMI (2019b); CPMI survey; national data.

① CPMI (2016).

Sources: Bech and Hancock (2020); HKMA (2020).

Box D

## Unified Payments Interface (UPI)

Unified Payments Interface (UPI), a mobile-based payment system, went live in September 2016 in India. In a short span of three years, the payments system has achieved a transaction count of more than a billion for three consecutive months, from October to December 2019, with volumes of 1.14 billion, 1.21 billion and 1.30 billion, respectively.

It is a 24/7/365 "fast payment" system via which users can send and receive money instantly using a Virtual Payment Address (VPA) set by themselves. It supports person-to-person (P2P) and person-to-business (P2B) payments, and can be used over a smartphone (app-based), a feature phone (USSD-based) and at a merchant location (app-based). It facilitates, among others, immediate money transfer through pull and push payments; merchant payments; utility bill payments; and QR code (scan and pay) based payments. It can also convey on-financial transactions such as mobile banking registration and balance enquiry.

The UPI framework comprises the National Payments Corporation of India (NPCI) as network and settlement service provider, banks as PSPs, banks as issuer and beneficiary banks, and third-party app providers such as Google Pay, Truecaller and WhatsApp. It powers multiple bank accounts into a single mobile application of any participating bank. Funds can be transferred using a VPA or account number with bank code (Indian Financial System Code, IFSC).

Transactions are executed on mobile devices with two-factor authentication using device binding and a UPI PIN as security. The UPI PIN is encrypted using public key infrastructure (PKI) technology. The UPI transaction data are stored in encrypted format in the app provider's system. The system was upgraded to UPI 2.0 in 2018 with a per-transaction limit of INR 200,000 and a few additional features related to customer convenience, safety and transaction security.

As of December 2019, 143 banks were live on UPI, including 21 public sector banks, 21 private sector banks, 50 cooperative banks, seven payment banks, seven small finance banks and 33 regional rural banks.

Leveraging the popularity of UPI, the Reserve Bank of India has provided an option to non-bank prepaid payment instrument (PPI) issuers to facilitate interoperability of their PPIs through UPI. The interoperability would be enabled for both the issuer and the acquirer side. This will give PPI holders access to all merchants, irrespective of whether they belong to a different PPI entity.

Source: Reserve Bank of India.

### 2.2.2 Central bank digital currencies

40. Digitalisation trends, among other motivations, have triggered a debate regarding the possibility that central banks could issue their own digital currencies – be it for wholesale or for retail use cases. For central banks in emerging market and developing economies (EMDEs), the financial inclusion potential is among the main reasons cited for analysing CBDCs (Boar et al (2020); see also Box E). For the purposes of this paper, CBDCs are referred to as a digital form of central bank money that is different from balances in traditional reserve or settlement accounts (CPMI (2018b)).

41. From an access and use case perspective, CBDCs can be restricted to monetary policy counterparts and other entities that have accounts at the central bank for wholesale payment and settlements, or they can be made available also to non-banks for retail payments. Only the latter scenario is directly relevant for this report. From the perspective of the transfer mechanism, CBDCs can be account-based or value-based. Payments with the former involve the transfer of claims recorded on an account operated by the central bank or a third party, similarly to reserve accounts and commercial bank deposits. In the case of value-based CBDCs, similarly to cash, payments are conducted on a peer-to-peer basis. At this early stage of CBDC exploration, it is not possible to determine what features – including the choice of transfer mechanism – best support financial inclusion objectives.

Box E

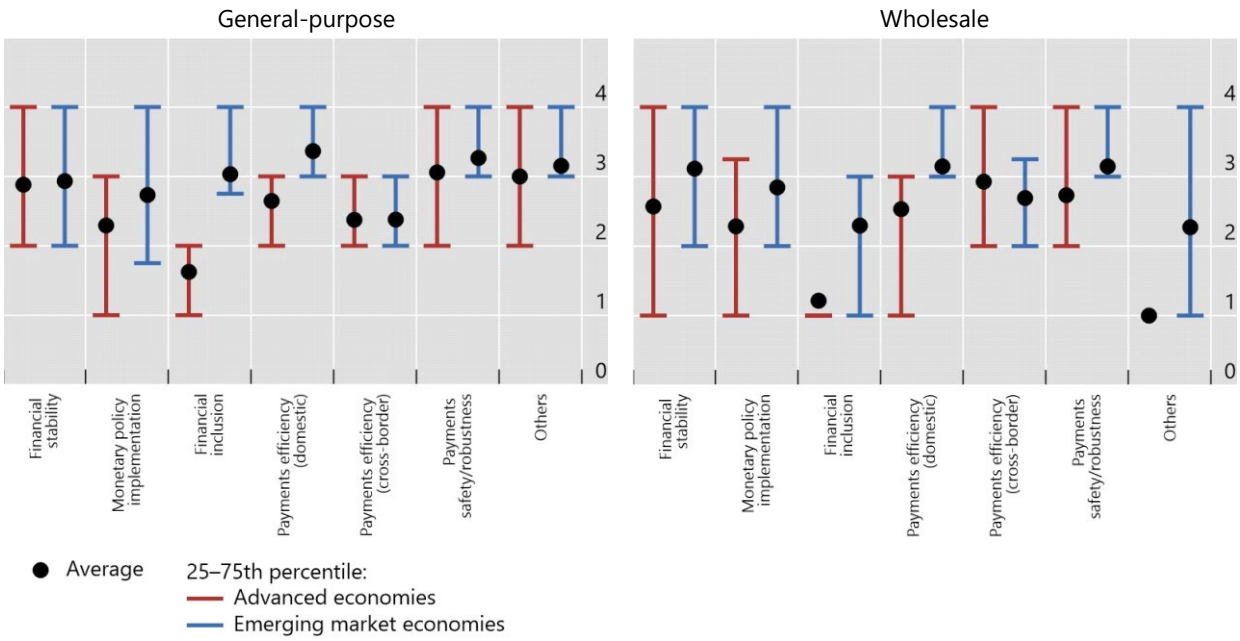
## Survey on CBDCs

The BIS-CPMI survey gives a global overview of CBDC work under way. Respondents from 21 advanced economies (AEs) and 45 emerging market economies (EMEs) have replied to the latest questionnaire. The updated results show that more and more central banks are researching CBDCs, with half focusing on both wholesale and general-purpose. About 40% of central banks are moving from conceptual research to experiments, and only a few EMEs have developed pilot arrangements.

Motivations for issuing a CBDC continue to be diverse. They are stronger for EMEs than for AEs (Graph E), in particular when a CBDC could be a complement to or a replacement for cash (left-hand panel). For EMEs, payments safety, domestic payments efficiency and financial inclusion are strong motivations for issuing a general-purpose CBDC. Domestic and cross-border payments efficiency are important drivers for researching wholesale CBDCs.

### Motivations for issuing a central bank digital currency

Distribution — Graph E




[1] "Not so important" (1); "somewhat important" (2); "important" (3); and "very important" (4).

Source: Central bank survey on CBDCs.

A rising number of central banks report that they are likely to issue a CBDC soon. Some 20% of 66 central banks said that they are likely to issue a CBDC within the next six years. EMEs indicate a higher likelihood to issue a CBDC than their AE peers. When queried on the legal authority to issue one, about a quarter of central banks stated that they have, or will soon have, such authority.

Meanwhile, private tokens remain a niche means of payment. The survey also asked central banks about stablecoins. Some 60% of them are looking into their monetary and financial impact. Those that are not considering the implications of stablecoins are mostly EMEs.

Source: Boar et al (2020).

### 2.2.3 Stablecoins

42. So-called "stablecoins" have evolved from the cryptoasset phenomenon, aiming to mitigate cryptoassets' volatility with a view to facilitating payments. Neither cryptoassets nor stablecoins are consistently defined. For the purpose of this report, cryptoassets such as bitcoin are value-based instruments (ie they are not based on accounts) which, unlike traditional instruments, neither constitute a financial claim on an issuer nor give rise to a proprietary right against an entity (ECB (2019a)). Cryptoassets aim to provide a solution to allow individuals and businesses to transact directly with each other without the need for a trusted third party by leveraging DLT. In practice, particularly because of their high price volatility, the use of cryptoassets as a means of payment is currently limited.[13] Stablecoins can be defined as digital units of value that are not a form of any specific currency (or basket thereof) and that rely on stabilisation tools to minimise fluctuations in their price relative to such currency/ies (Bullmann et al (2019)). To that end, stablecoins may resort to "backing" their value with fiat currencies or assets,[14] or attempt to match demand and supply to maintain parity with the reference currency/ies (ie algorithmic stablecoins). Depending on their design, stablecoins may or may not have a responsible issuer and/or disguise regulated functions. Compared with cryptoassets, stablecoins could be more capable of serving as a means of payment (G7 (2019)).[15]

43. Recent stablecoin initiatives have been sponsored by large technology and financial firms. With their existing large and often international customer base, these global stablecoin arrangements have the potential to scale rapidly to achieve a global or substantial footprint (G7 (2019)). Global retail stablecoin initiatives aspire to improve financial inclusion and facilitate cross-border payments. While it remains to be seen if and how global stablecoins can contribute to these policy objectives, they have prompted central banks in some countries to accelerate their investigations into CBDCs and generally resulted in greater attention being paid to the challenges of financial inclusion and more efficient cross-border payments (Feyen et al (2020)). No global retail stablecoin initiative is currently operational.

## 2.3 New access modes

### 2.3.1 Electronic wallets

44. Electronic wallets are payment arrangements that enable end users to securely access, manage and use a variety of payment instruments issued by one or more PSPs via an application (see also Section 2.3.3 on super apps) or a website. The electronic wallet may reside on a device owned by the holder, eg a smartphone or a personal computer, or may be remotely hosted on a server but is anyway under the control of the holder. This is irrespective of the underlying payment instrument used. Electronic wallets can support traditional payment instruments such as card payments, electronic funds transfers and e-money. They can also support new products that are not necessarily based on a transaction account, such as CBDCs, cryptoassets and stablecoins (see also Sections 2.2.2 and 2.2.3). Electronic wallets can facilitate both online payments and payments at the point of interaction.

[13] As of February 2020, some 16,000 retail venues worldwide were reported to accept major cryptoassets. BitPay and Coinbase, two of the largest processors of cryptoasset transactions, processed cryptoasset merchant payments worth USD 1 billion and USD 135million in 2019, respectively (Cuen (2020)).

[14] Traditional "off-chain" assets or "on-chain" assets / cryptoassets.

[15] Stablecoins could be designed for use by anyone (retail or general-purpose stablecoins) or only by a limited set of actors, eg financial institutions and their clients (wholesale stablecoins). For the purposes of this report, we take into consideration only retail stablecoins, whereas wholesale digital tokens are out of scope.

45. Thanks to increasing internet availability and growing smartphone adoption,[16] electronic wallets have gained traction worldwide. Prominent examples of electronic wallets with a global scale are PayPal, Apple Pay, Google Pay and Samsung Pay. Other electronic wallets have been issued by traditional PSPs, often on a local or regional level. The adoption of electronic wallets can be linked to financial inclusion gains via three mechanisms (Rolfe (2018)). First, insofar as the wallet's underlying payment instrument is based on a general-purpose transaction account, the increased popularity of electronic wallets may provide an incentive to open a transaction account, which is often a precondition for enjoying the wallet's full functionality. Second, electronic wallets enable a uniform and typically improved user experience,[17] irrespective of the underlying payment instrument, thereby encouraging the frequent use of transaction accounts. Third, in combination with contactless technologies, electronic wallets have a potential to fill the gaps in electronic payment acceptance in underserved (eg rural) areas and address the needs of small-scale businesses (Aveni and Roest (2017)).

46. Electronic wallets typically rely on tokenisation (Section 2.1.5 and Box A), and some use APIs to interface with the underlying account holding institution – eg Google Pay in India, which uses UPI.

### 2.3.2 Open banking

47. Open banking is defined as the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services and to initiate payments. Customer-permissioned data are retail customer data held by banks (eg customer transactions, personal identification data and customer financial history) that are permissioned by the bank's customer to be accessed by a third party (and possibly shared onwards with fourth parties). Individual jurisdictions may define open banking differently (BCBS (2019)).

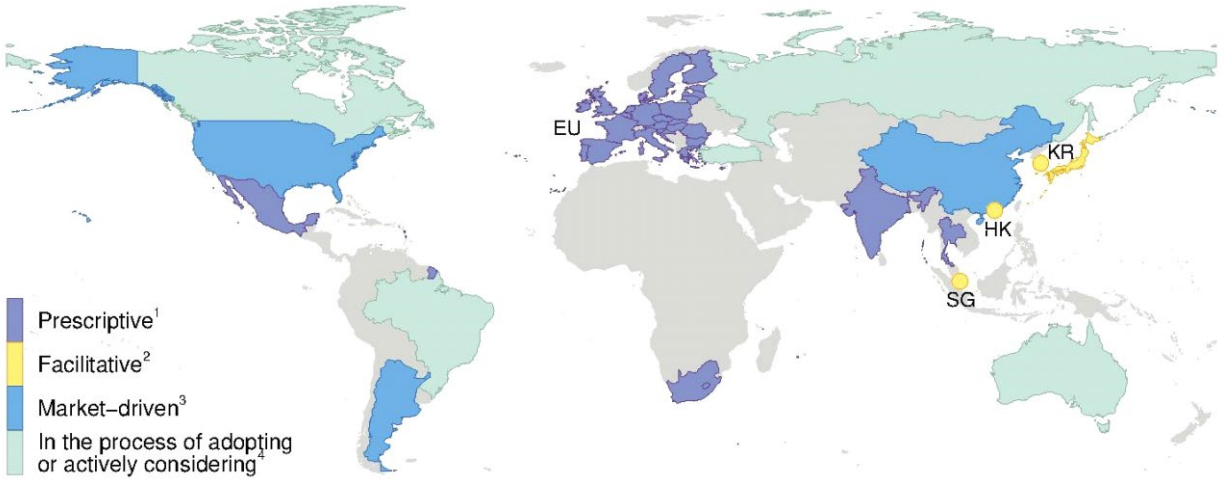
48. Open banking initiatives may vary from country to country with regard to their nature and scope. Some initiatives are driven by regulatory requirements (eg in the European Union) so that banks are required to share certain customer data with authorised third parties. These requirements may or may not include the use of a standardised, common API. Regulators' objectives include increasing competition and levelling the playing field for new market entrants, as well as fostering innovation. Other open banking initiatives are driven by the industry (eg in the United States) and/or championed by public authorities (eg in Singapore). With regard to the scope of the data shared, open banking initiatives may be confined to transaction account data only or extend to a broader range of financial accounts. Despite the fact that many financial institutions are still sceptical about giving third-party-controlled access to their customers' data, some banks see moving away from a closed environment as an opportunity too (Wiebusch (2017), PWC (2018)).

[16] GSM Association estimates that smartphones represented 60% of total mobile connections in 2018 and are predicted to increase to nearly 80% by 2025. The adoption rate in South Asia and Sub-Saharan Africa was 48% and 39%, respectively. As they become more affordable and achieve longer battery life, the adoption and use of smartphones and other data-enabled devices is likely to increase. Although affordability (or lack thereof) remains an important consumer barrier, the average monthly cost of a 500 MB data plan fell from 4.8% to 2.5% of monthly GDP per capita between 2014 and 2017, whereas the average cost of an entry-level internet-enabled device fell from 2.6% to 2.3% of GDP per capita (Bahia and Suardi (2019)).

[17] Mobile money has been credited with a large share of the financial inclusion gains over the past years. According to GSM Association, there are currently 272 live mobile money deployments in 90 countries (GSMA (2019b)). However, many mobile money accounts are dormant. Reasons for this might be negative user experiences with mobile money accounts being based on long USSD menus and the limitations of features phones when it comes to the user interface. These challenges can be overcome through the increasing adoption of smartphones and electronic wallets (Chen et al (2016)).

Approaches to open banking across the globe

Figure 3




The boundaries shown and the designations used in this map do not imply official endorsement or acceptance by the BIS.

EU = European Union; HK = Hong Kong SAR; KR = Korea; SG = Singapore.

[1] Requires data-sharing. [2] Encourages data-sharing. [3] No explicit rule/guidance requiring data sharing. [4] In the process of adopting or actively considering adopting.

The FPSs in Aruba, Bahrain, Hong Kong SAR and Singapore are represented by circles.

Source: BCBS (2019)

49. While open banking initiatives target traditional bank accounts and can be leveraged to initiate instant payments or traditional credit transfers, mobile money providers in selected markets are also establishing payment platforms with access via APIs. For example, Safaricom M-Pesa in Kenya or MTN in Uganda are offering API portals for businesses and/or third-party developers to enable mobile money to be integrated into service offerings (eg PAYG energy solutions and personal financial management solutions).

Box F

## Approaches towards open banking in selected jurisdictions

In Australia, open banking is the application in the banking sector of a comprehensive consumer data right act (the Treasury Laws Amendment (Consumer Data Right) Act 2019) that also encompasses the energy and telecommunications sectors, and will be rolled out economy-wide on a sector-by-sector basis. In a nutshell, the Consumer Data Right Act gives consumers the right to safely access certain data about them held by businesses and enables the transfer of those data to accredited third parties of their choice such as comparison websites. This should improve consumers' ability to compare products and services as well as their capacity to either negotiate better deals with their current providers or switch providers. Over the longer term, this Act is expected to promote consumer-centricity, encouraging the development of new products and applications that reach more consumers and are better tailored to their needs. Notably, the Act includes a principle of reciprocity, which provides that those who wish to become accredited and receive designated data at a consumer's request must be willing to share equivalent data, in response to a consumer's request.

The Canadian government is undertaking a review of the merits of open banking, having appointed an Advisory Committee on Open Banking in 2018. Advisory Committee members will represent the broad interests of Canadian society. In a first phase the Committee would assess the merits of open banking, followed by an assessment of implementation considerations in a second phase in 2019.

In Japan, open banking was announced in the government's "Growth Strategy, 2017". While it is on a voluntary basis, the government was committed to have more than 90 banks offering open APIs by 2020. If banks decide to opt in, they must comply with specific rules.

In India, the Reserve Bank of India has provisionally licensed over half a dozen account aggregators and released a first set of technical specifications required for all entities (eg banks, insurance companies, goods and services tax platforms) seeking to participate in the proposed account aggregator ecosystem. Based on these technical specifications, authorised providers can offer apps, enabling customers to aggregate a variety of data (eg payment patterns, tax returns) that they can then choose to share instantly and temporarily with service providers.

In Hong Kong SAR, the Hong Kong Monetary Authority (HKMA) published an Open API Framework in 2018 to encourage banks and third parties to work together to develop innovative banking services to improve customer experience. Open APIs are being implemented in four phases: product information (Phase I); customer acquisition (Phase II); account information (Phase III); and transactions (Phase IV). Under Phase I (January 2019), 20 banks opened up some 500 Open API end points, covering information on over 1,000 products and services. Under Phase II (October 2019), the banks also provided about 300 Open API end points supporting applications for various banking products and services. The HKMA considers it desirable to define a more detailed set of standards for Phases III and IV to facilitate secure and efficient implementation across the industry before setting out a concrete implementation timetable for those phases.

Sources: Australian Treasury (2019); Department of Finance Canada (2019); Manikandan (2019); Rai (2020); HKMA.

### 2.3.3 Super apps

50. Super apps provide end users with a one-stop shop for a variety of services and are typically offered by big tech companies, ie large companies with an established technology platform. While these big tech companies often start with single-purpose apps (eg for messaging, e-commerce, ride hailing, lodging), they are continuously incorporating additional services, including payment and other financial services. Super apps create an ecosystem that connects a large number of individuals and/or firms, thus generating network effects and economies of scale that allow costs to be lowered and processes to be improved. By expanding the service offering beyond the core product, super apps are aimed at increasing customer loyalty, the ultimate goal being repeat end users that spend as much of their online time as possible within the super app. This stickiness can affect market entry, since it can be difficult for end users to change to another super app or to multihome (D'Silva et al (2019), FSB (2019d), King (2019), Ruehl and Kynge (2019), Zhang and Chen (2019)).

51. Providers of super apps have an interest in their users being able to transact seamlessly by integrating a variety of electronic payment instruments within their apps. Some providers have launched their own payment scheme and/or support users in gaining access to transaction accounts. These efforts are aimed at fully integrating payments into the core business services and enabling end users to initiate and receive payments within the provider's ecosystem. These types of payment are often referred to as embedded payments. If the provider does not offer payment services on its own to end users, the super app allows the customer's payment details to be stored (increasingly through tokenisation) or APIs to be used to interface with the institution holding the customer's account, thus enabling the customer to benefit from fast and largely automated checkout systems. Super apps may in future support so-called invisible payments, where end users pay in physical stores without presenting a physical payment instrument or mobile phone at the checkout or terminal.[18]

52. Super apps have to date been especially popular in China, where Alipay and WeChat Pay have succeeded in establishing a large and highly engaged customer base and expanding into financial services beyond payments. Another relevant example is Grab, currently offered in eight countries and more than 300 cities. Several other solutions have a dominant share domestically. Prominent examples are Go-Jek and Ovo in Indonesia, Boost in Malaysia and KakaoPay in Korea (BCG (2019), King (2019), Ruehl and Kynge (2019)).

53. Financial services beyond payments include loans and insurance for small businesses (Grab) and consumer credit (Go-Jek). Providers typically use the data generated via these super apps, including non-financial data, for their underwriting decisions (Ruehl and Kynge (2019)). With increasing success and/or due to legal and regulatory requirements, some providers of super apps have spun off their payment and/or financial services into separate entities offering financial services (including payments), while still being technically fully integrated in the super app.

[18] These solutions (eg Amazon Go) use new technologies such as computer vision, deep learning algorithms and sensors to detect which items have been removed from the shelves, or turn the payer's mobile phone into a checkout device for scanning items (eg Barclay's Grab+Go) and, upon the customer leaving the store, initiate the payment based on the payment details on file.

# 3. Opportunities and challenges of fintech developments in driving access to and usage of transaction accounts

54. The PAFI report identified four "catalytic pillars" as drivers of access to and usage of transaction accounts, namely: (i) transaction account and payment product design; (ii) readily available access points; (iii) awareness and financial literacy; and (iv) leveraging of large-volume recurrent payment streams. This section aims to determine whether and how the fintech developments described in Section 2 can boost these drivers.

55. For each of the drivers, this section provides examples of how new technologies – and the new products, services and access modes these technologies underpin – can help resolve outstanding challenges and barriers. Through these examples, it is possible to identify four broad groups of potential benefits of fintech: (i) efficiency gains for service providers and system operators; (ii) market contestability; (iii) user experience; and (iv) ubiquity. The analysis also shows that fintech developments thus far are not suited to support all drivers equally. Fintech seemingly offers the most benefits for transaction account and payment product design and for readily available access points, whereas it currently plays a lesser role in the areas of awareness/financial literacy and large-volume recurrent payment streams.

56. It should be noted that fintech developments are by their very nature new and/or untested, and may present challenges that, if not properly identified and addressed, could undermine the PAFI objectives. The analysis shows that, for each identified benefit, there are some drawbacks. Potential risks resulting from fintech developments relate to: (i) safety, including cyber resilience; (iii) consumer protection and data privacy; (iii) market concentration; and (iv) digital exclusion. These risks highlight the importance of effective regulatory, oversight and supervision frameworks in the broader context of the PAFI foundations (Section 4).

## 3.1 Transaction account and payment product design

### 3.1.1 Instant payments satisfy the demand for greater speed and end user control

57. Rapid technological change in daily life has also altered end users' expectations of payment service features, specifically with regard to speed and availability. Instant payments allow evolving end user needs to be met by enabling individuals and businesses to make and receive payments at any time, in (near) real time. Designed to ensure funds availability in the payee's account within seconds and to process payments on a 24/7/365 basis, instant payment solutions enable the transfer of money to friends and family "on the spot", and access to accounts at any time, among other things.

58. Many instant payment implementations enable the payee to send a "request to pay" message to the payer, combining features of a direct debit with the benefit that it is still up to the payer to initiate that payment by confirming the push notification received on their device. Request-to-pay messages can be earmarked for a dedicated purpose (eg school fees or utility bills). The funds received could either be transferred directly to the school or utility service provider or credited to a dedicated account (eg M-Tibia offered by Safaricom and PharmAccess, where end users receive conditional health payments into a specialised wallet) (Mihet (2019)).

59. Instant payments can also endow their users with the ability to better control their finances. Instant funds verification can reduce the likelihood of end users running unintentional overdrafts and help them avoid costly short-term financing. On the receiving side, the close-to-immediate availability of funds offers an alternative to cash payments and may be helpful if there is a need for emergency spending. It is worth noting that most instant payment solutions are designed as push transactions (ie payers initiate

and/or approve the payment before their account is debited). This gives end users more control over their funds than with pull payments (such as card payments and direct debits).[19]

60. For instant payments to fulfil the needs of the financially unserved and underserved, they need to provide a close substitute for cash and act as a gateway product towards other financial services by being based on a general-purpose transaction account. With regard to the former condition, in principle, instant payment implementations already allow the immediacy of cash to be matched. However, to serve as a (close) substitute for cash, instant payments would also have to be as widely accepted, cater to a wide range of use cases beyond P2P payments, be affordable, and be easy to use.

61. In a person-to-business (P2B) payment context, instant payments allow merchants to enhance their cash flow management**.** Once the funds have been credited to the merchant's account – within seconds of the customer initiating the payment – such payment is final and cannot be reversed. Because the merchants do not face the risk of a customer's payment failing, they may release the goods/services more quickly, thereby improving their customers' experience without the need to rely on a payment guarantee by the PSP. Unlike in the case of card payments, businesses receiving instant payments usually benefit from having immediate access to their funds, while also avoiding the costs and risks associated with the handling of cash.

62. Compared with traditional card payments, instant payments can reduce costs by enabling point-of-interaction payments without the need for traditional payment acceptance infrastructure. At the point of interaction, some instant payment solutions incorporate the use of mobile channels and contactless technologies (eg QR codes) that do not rely on the traditional electronic payment acceptance infrastructure (eg physical payment terminals) but rather on the merchant's (and/or customer's) smartphone (eg to display or read QR codes, or a printout of the merchant's QR code identifier; see also Section 3.2.2). It is worth noting, though, that any savings and other advantages that derive from the use of alternative acceptance infrastructure are not specific to instant payments and may not eliminate the need to support conventional card acceptance infrastructure, adding complexity for the merchants.

63. Furthermore, merchants may benefit from lower merchant service charges. In principle, instant payments could be free of charge for the merchants if the costs were shifted onto the payer, but this may not be possible in all circumstances and may be considered as detrimental to the acceptance of instant payments by payers. UPI in India uses a standard four-party scheme interchange model, albeit with lower interchange fees compared with card payments. Lower merchant fees may be of a temporary or a permanent nature. For instance, merchants may be exempted or benefit from reduced fees to promote the acceptance of instant payments compared with card payments. Lower overall costs for PSPs might allow them to offer a lower merchant service charge in the long run, since some of the cost elements of card payments, such as payment guarantee or repudiation-related chargebacks, are typically not relevant for instant payments. It should also be noted, however, that increasingly card payments have been the object of initiatives to regulate interchange fees (eg in Australia, the European Union and the United States), which may result in downward pressure on merchant fees for card payments too.

[19] In this regard, the Better than Cash Alliance (BTCA) and the Global Partnership for Financial Inclusion (GPFI) recommended that fast payments be implemented as push payments only in order to limit the risk of unauthorised debits.

Box G

## Leveraging instant payments for P2B uses cases – the Mexican example

The Bank of Mexico, together with the payments industry, has developed Cobro Digital (CoDi), which was rolled out in October 2019. CoDi offers payees (mainly small and micro-merchants, e-commerce merchants, and individuals) a viable alternative for accepting and receiving electronic payments safely and in a cost-effective and transparent manner via an app on their mobile devices. It is expected that ease of use and wider acceptance may lead more individuals, especially small entrepreneurs, to open an account in order to receive CoDi payments. Payments are initiated via QR codes, NFC or instant messages, and funds are transferred via the interbank electronic payment system (Sistema de Pagos Electrónicos Interbancarios, SPEI), thereby making this core infrastructure available to any payer. CoDi will compete with other payment methods that are suitable for P2B-type payments such as payment cards, and in particular with debit cards. In this regard, the advantages of CoDi include the real-time availability of funds for the merchant (compared with next-day availability or longer for payment cards), reduction of fraud, a low and fixed cost per payment received, and much lower initial investment and maintenance costs.

Source: World Bank (2019c).

64. On the other hand, fund availability within seconds of payment initiation makes instant payments an attractive option for fraudsters. Payers, especially from more vulnerable groups, might be manipulated to authorise payments to the wrong payee and/or for a wrong amount. Fraudsters make use of the same features of instant payments as legitimate end users do. If the victim can be convinced to transfer the funds via instant payments, this increase the likelihood that fraudsters can quickly withdraw funds before the fraudulent activity is spotted.[20] Risk mitigation strategies include the attempt to reduce the potential damage by imposing limits on the amount of individual transactions, imposing cooling periods after the addition of new beneficiaries (eg transfers can only be initiated 30 minutes after the addition), requiring the payer to verify the name of the payee as an additional authorisation step and/or conducting velocity checks for beneficiary additions and transactions. Big data analytics such as machine learning could be useful to detect fraud in real time, eg by identifying untypical payment patterns conducted via certain transaction accounts (for additional measures, see Box H).

Box H

## Measures to mitigate fraud attempts that leverage instant payments

In addition to state-of-the-art processes for customer onboarding and the related KYC checks, PSPs can enhance customer behaviour profiling, conducting (technical) front-end profiling of customer usage patterns for mobile devices, browsers etc, covering a large number and wide range of technical attributes, (business) back-end profiling of customer transactions and additional third-party provider profiling.

PSPs can centralise fraud alert handling and customer interaction in a dedicated 24/7 specialised team focusing both on (instant) payments and on card payment fraud. This centralisation effort should ideally also involve the setup of one central risk engine for profiling and scoring transactions across services, contributing to more effective fraud profiling and scoring and helping to avoid the proliferation across multiple channels of fraud cases related to the same customer.

[20] Comparable figures on this type of fraud are currently not available. In 2017, UK Finance registered 43,875 fraud cases where the payer was manipulated to authorise a payment of the wrong amount and/or to the wrong payee. The resulting total losses in the United Kingdom amounted to GBP 236 million (FCA (2018)).

PSPs need to develop the necessary abilities to detect and distinguish scam and fraud, and can benefit from implementing automated, real-time fraud detection features (especially for instant payments – ideally prior to strong customer authentication), enhanced monitoring of both incoming and outgoing payment flows on customers' payment accounts, and the introduction of two-factor authentication solutions that are both risk-based (establishing fraud risk based on technical attributes) and dynamic (eg not always requiring the same sequence of two-factor authentication steps). Finally, PSPs need to ensure that customers are made aware of and educated about fraud-related risks and prevention measures.

On a payment infrastructure level, a central fraud scoring solution at PSP level – potentially within an entire region – allows the payer's PSP to provide a fraud score for outgoing payments, preferably in the payment message itself, to support the payee's PSP in its inbound fraud detection activities, without entailing any liability shift. Such solutions are currently being piloted or pioneered at national level in different communities. The definition of a "request for blocking of beneficiary account" message, and fraud investigation/information messages in ISO 20022 format, could serve as a more effective alternative to an emergency contact list in the event of scam/fraud-related issues causing the cancellation. In addition, agreeing on a set of data elements and a related ISO 20022-based transmission format for the exchange of contextual information (eg the information that this is the first time this payer is sending a payment to this payee account) between the payer's PSP and the payee's PSP can facilitate fraud detection activities at beneficiary PSP level. Finally, the definition and implementation of supportive fraud detection measures at central infrastructure level – to identify, for instance, fraud-related funds transfers across financial institutions, eg cashouts based on consecutive instant payments from one account to the next – and the establishment of a forum to enable the exchange and discussion of recent and relevant fraud case experiences and the communication of any related conclusions or guidance to relevant stakeholders can further mitigate the risks of fraud leveraging instant payments.

Source: Euro Banking Association (2019).

### 3.1.2 Open banking has the potential to augment the usefulness of transaction accounts

65. By allowing authorised third parties to access PSP customer data, open banking may result in new and improved services being made available to individuals and firms.[21] By gaining insights into customers based on data held by the respective account-servicing PSPs, third-party providers may be able to create new propositions that increase the usage of transaction accounts, eg by initiating credit transfers to online merchants. By breaking down data silos within and across PSPs, open banking could also provide a pathway to broader financial inclusion for the currently underserved by enabling new providers to offer savings, investment or insurance products that cater to the customers' specific needs. At the same time, through open banking, banks can personalise and expand the range of products they offer to their customers.

66. Open banking may make it easier for customers to access and compare competing PSP offers and hence to switch between providers according to their personal needs. In turn, this may increase transparency and competition to the benefit of end users (eg by enabling better price comparison services based on consumers' actual usage) (UK Finance (2018)). In open banking environments, users may gain a consolidated view of their accounts/finances. If users are better informed about their financial situation, they may be able to avoid costs, eg from overdrafts, and manage their finances more effectively, including increased transparency on idle balances and taking advantage of additional services such as budgeting tools and categorising spending. However, data from the Netherlands show that only a minority of consumers would give consent to the usage of payments data in order to receive a financial overview with personalised offers, unless they are offered an explicit financial reward (Bijlsma et al (2020)).

[21] The scope of customer data accessible by authorised third parties may vary depending on the country's implementation/legislation. For instance, in Europe open access is limited to payment account data excluding other accounts (eg credit cards).

67. Open banking does not come without risks, though. The greater flow of customer data between the entities involved in open banking can exacerbate data security concerns. Open banking expands the attack surface and can increase the likelihood of data breaches that can potentially expose customers' sensitive information and lead to identity theft and subsequent financial losses for customers. Risks vary depending on the business model and functioning of the open banking model. Services provided by third parties that entail the effective transfer of funds (eg payment initiation services that involve funds transfers based on the data retrieved from the customer) come with greater risks than data aggregation or account information services. Furthermore, the access or communication mechanism between the PSP maintaining the transaction account and the third parties affects the level of data security risks (eg screen scraping gives access to all data a customer themselves can see via online banking as compared with dedicated interfaces via API that can limit the data points third parties are allowed to see).

68. Uninformed consent to the use of personal information for open banking may put customers at risk. Studies show that up to nine out of 10 end users do not even read terms and conditions before accepting them. Consent alone is therefore not enough to protect end users and to serve financial inclusion purposes. Open banking initiatives need to carefully consider the way consent is obtained, and providers need to take responsibility to ensure that access by non-authorised entities is prevented and that authorised ones strictly adhere to the rules (eg to avoid that more information than absolutely needed is obtained via open banking access, such as the consumer's spending habits) (IIF (2018), Murthy and Medine (2018), Australian Treasury (2019)).

### 3.1.3 Digital ID simplifies customer due diligence

69. The PAFI report refers to cumbersome and costly customer due diligence (CDD) requirements as one of the factors constraining PSPs' ability to strike a balance between costs and functionality and to design transaction accounts that meet the needs of the target population. Digital IDs can help financial institutions comply with the customer identification and verification components of CDD (Natarajan et al (2018)).

70. First, digital ID supports e-KYC processes, thereby lowering transaction costs for providers through the near elimination of paperwork as well as the burden of keeping paper records, and facilitating audit and forensics through the electronic storage of information.[22] From a user perspective, cost savings can be passed on to consumers through lower fees; furthermore, new clients may find the process of opening an account less cumbersome when it entails e-KYC instead of paper-based documentation (AFI (2019), Kipkemboi et al (2019)).

71. The availability of a digital ID that allows customer identification and verification needs for a basic account to be met as well as limits to be enforced (on the number of accounts, value of transactions) can motivate financial sector regulators and public authorities to simplify the CDD requirements (Natarajan et al (2018)). Where implemented, tiered KYC regimes have produced positive outcomes on the target segments (AFI ((2018)). The Financial Action Task Force (FATF) has developed guidance to clarify how digital ID systems can be used for CDD. The guidance is intended to help governments, financial institutions and other relevant entities apply a risk-based approach to the use of digital ID for CDD (FATF (2020)).

72. A digital ID can also support the establishment of KYC registries – centralised repositories of CDD records of customers in the financial sector (Natarajan et al (2018)). KYC registries allow inter-usability of the CDD records across the sector with the objective of reducing the burden of producing and verifying CDD documents each time the customer creates a new relationship with a financial entity. From a user

[22] Provided the legal framework does not prescribe, or can be interpreted as prescribing, hard copy formats.

perspective, an existing customer does not need to go through the burdensome process of submitting various documents to prove their identity repeatedly.

Box I

## India's e-KYC approach

India's Aadhaar ID system includes an e-KYC service to expedite the verification of a client's identity. The e-KYC service enables an individual with an Aadhaar number to allow the Unique Identification Authority of India (UIDAI) to disclose the individual's personal information to service providers that wish to instantly activate services such as mobile plans and bank accounts. The Aadhaar-based e-KYC process is paperless, consent-based, private and instantaneous. As a result, reliable CDD data can be shared in real time, but will only be released directly to service providers upon the consent of the customer so as to protect an individual's privacy. Around 5 billion e-KYC transactions have already been executed through Aadhaar. Going forward, the Central KYC Records Registry (CKYCR) is envisaged as a repository of the KYC records obtained by service providers across the financial sector. This database will enable inter-usability of the KYC records with the goal of making the CDD process more efficient for the financial sector.

Source: Natarajan et al (2018).

73. Because these approaches rely on a digital ID, they are also exposed to risks that are inherent in the underlying digital ID infrastructure, including data breaches and cyber attacks, and concerns over the control and misuse of personal data, as well as flawed infrastructure's design, for instance with regard to governance, access, population coverage, data quality, connectivity/offline capabilities (Kipkemboi et al (2019)) and interoperability (see also Section 4.3.3).

74. DLT may further support inter-usability of CDD records between organisations and across borders. Decentralised identity verification solutions based on DLT could provide similar benefits for PSPs in terms of CDD efficiency as centralised registries, and bring potential benefits in terms of resilience, data integrity and individuals' control over the use of their identity.[23] However, at this stage, these developments are not yet mature for large-scale applications, and potential legal risks would need to be addressed (World Bank (2018b), Natarajan et al (2018)).

### 3.1.4 The design of central bank digital currencies can aim at providing universal access to a basic means of payment

75. Central banks around the world are assessing the costs and benefits of issuing CBDCs for a variety of reasons, including improving financial inclusion. Surveys show that the central bank community maintains a strong interest in exploring the option of issuing CBDCs, with domestic payments efficiency, payments safety and financial inclusion, on average, all considered "very important" in this respect for EMDEs. Advanced economies are considering the need for an alternative, robust and convenient payment method in the event of a considerable reduction in the use of cash as a factor when exploring CBDCs (Boar et al (2020), IMF-World Bank (2019)).

76. Even though interest is high and conceptual development is ongoing, apart from some pilot projects, CBDC so far has not been issued on any operating, live network. In fact, the complexities associated with CBDC implementation require careful consideration of both benefits and costs. However, central banks representing a fifth of the world's population state that they are likely to issue the first CBDCs in the next few years (Boar et al (2020)).

[23] Self-sovereign identity (SSID) is a mechanism which allows an individual/entity to assert their own identity without having to rely on any third party by simply proving that they have control over the private key that corresponds to the linked identity transactions, and to divulge only that information that needs to be shared with the service provider.

77. CBDCs could be designed to ensure access to a basic, trustworthy means to pay and store value in situations where PSPs do not offer transaction accounts that effectively meet the needs of the unbanked and/or have failed to instil trust. Notwithstanding the role of new technologies in enabling PSPs to enhance transaction accounts and payment product design, PSPs may still face challenges in meeting the needs of the target populations at little or no cost. For instance, the PAFI report sheds light on the somewhat limited availability and use of basic accounts owing in part to thin profit margins for their providers, and little scope for (higher-profit-margin) product cross-selling to basic account holders. Lack of trust might be motivated by unstable banking systems and/or a perception of transaction accounts being unsafe due to high incidence of fraud.

78. Where access to cash is cumbersome, CBDCs could be designed to replicate certain cash-like attributes to ensure that individuals and businesses have access to a simple, risk-free and flexible means of payment. Accessing cash (which typically relies on bank infrastructure such as branches and ATMs) might be challenging and/or costly in remote areas (eg small islands, difficult-to-reach regions). Cash logistics might be especially difficult in the event of natural disasters or conflicts. While a CBDC may be designed to overcome such issues, it might not offer the level of privacy guaranteed by physical cash. Balancing privacy and other public policy objectives such as financial integrity is one of the challenges with respect to CBDCs (ECB (2019b)).

79. Ultimately, the benefits of CBDCs aimed at providing universal access to a basic means of payment must be weighed against the costs and any challenges for other policy areas (eg monetary policy transmission, financial intermediation and financial stability). A central bank may face additional operational and reputational risks, including from using new technologies on a scale yet to be tested, when issuing a CBDC. Finally, there is also the risk that CBDCs may duplicate or crowd out private sector initiatives that could be equally or even better suited to provide individuals with a basic means of payment, such as an industry-wide instant payment scheme. In conclusion, while CBDCs could be designed with financial inclusion in mind and to mitigate challenges for other policy areas, if the main objectives are access to and usage of transaction accounts, CBDCs are not likely to be the first or most straightforward choice for the time being.

### 3.1.5 Super apps cover a wide range of payment needs in their users' daily lives

80. Super apps facilitate a wide range of tasks in their users' daily routines (eg ride hailing, hotel booking, ticketing, appointments and payments). Attracted by the convenience, ease of use and discounts, users have an incentive to open transaction accounts (either at a financial institution or in the super app) as a requirement to access full-fledged services in the app. The link between users' (digital) lives and payments as well as other financial services is apparent also in both the increasing role of social media and instant messaging platforms (in financial services and the growing use of social media by financial institutions (Shrader (2014)). Given the sheer size of social media user bases and the number of use cases enabled by super apps, the potential impact on both access to transaction accounts and their frequent usage could be substantial. Super apps imply users' access to the internet and a smartphone, for which reason the availability and affordability of information and communication technology play a critical role.

81. However, the digital divide, including the digital gender divide and digital use divide, is still prominent globally and particularly affects underserved and unserved people. Despite some promising developments, affordability (or lack thereof) remains a key barrier, especially in middle- and low-income countries. Furthermore, women are on average 10% less likely to own a mobile phone, and 26% less likely to use mobile internet than men (Rowntree (2018)).

## 3.2 Readily available access points

### 3.2.1 New products and services change the demand for physical access points and cash

82. New products and access modes may result in fewer readily available access points such as bank branches or ATMs. Traditional banks are expanding their digital banking services while simultaneously reducing their physical presence. At the same time, virtual banks (Section 4.2.1) often have no physical presence at all. In both cases, technological innovation has helped cut operating costs, whether related to headcount or to physical infrastructure. As the network of physical access points becomes less dense, consumers are increasingly steered towards the use of remote access channels.

83. Smartphone penetration rates are increasing worldwide, but mobile data infrastructure is often not keeping pace and/or data packages are too expensive for underserved and unserved customers, especially in EMDEs and specifically in rural areas. End users might therefore only be able to use fintech innovations relying on mobile data sparingly – if at all. Some innovative products and services try to address this challenge by having apps that use less data or even use USSD infrastructure where connectivity is low (Murthy et al (2019)).

84. Both the rapid digitalisation of payments and a reduced physical presence of PSPs could negatively affect the availability and acceptance of cash, and ultimately deter certain segments from acquiring, maintaining and using transaction accounts. The availability and acceptability of cash require its physical production, its distribution by the private sector – banks and ATM providers – and merchants to accept it. The declining use of cash means loss of economies of scale, and early examples can be observed where cash is no longer accepted and only electronic payment can be used[24] (BoE (2020)).

85. With fewer options available to access cash,[25] consumers are expected to increasingly use digital payment services. However, without convenient access to and acceptance of cash, there is a risk that some segments will be left (further) behind, including senior citizens, individuals with disabilities, undocumented migrants, people living in, or moving out of, extreme poverty or homelessness, the inhabitants of rural and remote areas, and those with limited financial capability (Access to Cash Review (2019)). For a variety of reasons (including challenges of access to transaction accounts as identified in the PAFI report), these groups rely on cash and would have difficulty coping with a cashless society (Sveriges Riksbank (2018)).

86. Growth in e-commerce and higher acceptance of electronic payments by physical retailers also reduce the need for cash. While the majority of merchant payments – especially in the case of micro-, small and medium-sized retailers – are still made in cash, there is a clear trend towards electronic payments and in a number of countries card payments have already exceeded cash payments in terms of value or volume. This trend can, for instance, be observed in Denmark (Danmarks Nationalbank (2017)), Estonia (ECB (2017)), Germany (EHI (2019)), the Netherlands (DNB-DPA (2018)), Norway (Norges Bank (2019)), Russia (Finextra (2020a)), Sweden (Sveriges Riksbank (2019)) and the United Kingdom (Peachey (2019)).

87. In many EMDEs, the use of new products and services (including mobile money and other electronic forms of payment) for merchant payments might be a challenge for the traditional mobile money agent remuneration model. This model relies on a variable commission basis, with cash-in/cash-

[24] While, for example, 3.4 million people in the United Kingdom rarely use cash, 2.2 million people rely almost wholly on cash, up from only 1.6 million in 2014 (Greenham and Travers-Smith (2019)).

[25] The UK consumer association Which? found that, between January 2018 and end-2019, more than 8,700 fee-free ATMs were either closed or converted to fee-paying, with the consequence that people living in rural areas have to travel three times further to find an alternative fee-free ATM than they would if they lived in a town or city. The amount paid by consumers to withdraw cash jumped by GBP 29 million to GBP 104 million in 2019, with fee-charging ATMs typically having a GBP 2 per-transaction price point (Robbins (2019), Shaw (2019), Finextra (2020c)).

out transactions (CICO)[26] being an important component. In order to maintain a sustainable network of active agents, especially in rural areas, service providers may need to review and improve their agent business models, eg by enabling agents to generate more revenue streams from different types of transactions from financial and non-financial services (Hernandez (2019)). New products and services have also resulted in the emergence of specialised entities providing services to unify the processes across different types of payment products (payment gateways) and support acquiring PSPs in servicing smaller merchants (payment aggregators).

Box J

## Leveraging big data analytics for optimisation of agent networks

Data analytics can be leveraged to improve agent networks in terms of geographical coverage and gender balance. Based on transaction and geolocation data, PSPs aim to identify an optimal distribution of physical outlets, ATMs and/or agents, and to enhance liquidity distribution among PSP agents and predict their need for cash.

In the Democratic Republic of the Congo, a gender-sensitive analysis of the country's agent network was conducted by the microfinance institution FINCA in order to determine whether there were significant differences between male and female agent constraints and performance. Based on the findings, a targeted recruitment of more women as agents was started and the liquidity distribution optimised to cater for the types of transactions female agents mainly facilitate.

Sources: GSMA (2018b); Hernandez (2019).

### 3.2.2 Electronic wallets in combination with contactless technologies can expand the number of acceptance points at low cost

88. New technologies, often in combination with new products and new providers, blur the line between in-person and remote payments. The PAFI report classifies service points and access channels on the basis of how payments are initiated from the payer's perspective, with the two main types of payment initiation – in-person payments and remote payments. In particular, POS terminals were considered as access points for in-person payments (together with bank branches, ATMs, PSP agent offices, etc), whereas the mobile phone network was regarded as an access point for remote payments.

89. Contactless technologies, and especially QR codes, offer a low-cost alternative to traditional POS terminals by leveraging the mobile (smart) phone channel. While plug-in devices for mobile phones have been offered for several years now, they were mainly limited to markets with a high penetration of payment cards. QR codes offer a new alternative, by lowering hardware requirements on the payee, and decreasing the operating costs of acquirers. Payees without a smartphone can also accept electronic transactions by simply displaying a printout of the QR code for the payer to scan (Chiampo et al (2018)). Much of the success of Alipay and WeChat Pay acceptance is attributable to the QR code feature (CGAP (2019)). In India, Paytm is now processing a substantial volume of merchant payments based on QR codes.[27] Even in markets with a high penetration of payment cards, POS terminals are used to display QR codes (eg in Switzerland).

90. Technologies such as tokenisation and biometrics that are used in electronic wallets and contactless payments have the potential to enhance security by making it harder for criminals to obtain

[26] CICO refers to the process whereby customers deposit/withdraw cash in/from their transaction accounts in order to access the payments system. CICO networks provide these services via bank branches, ATMs and individual money agents.

[27] India has announced that a Payments Infrastructure Development Fund (PIDF) would be created for increasing the acceptance infrastructure of physical and digital POS. Contributions to the fund will be made by the RBI, card issuers and card networks; the fund will be administered by the RBI.

sensitive payments data and/or commit payment fraud (Danmarks Nationalbank (2017)). At the same time, the increased popularity of QR code payments has resulted in new fraud patterns in some countries. Static merchant QR codes can, for instance, be easily replaced by fraudulent QR codes that redirect payments to the fraudsters' accounts or other unsafe sites. The People's Bank of China has issued regulations that cap individual QR code payments at CNY 500 (roughly USD 70) per day, with the option of increasing this limit to CNY 5,000 when security factors, such as digital certificates and electronic signatures, are implemented. The Reserve Bank of India has included the enhanced usage of signed and encrypted Bharat QR[28] as a preventive measure for secure payments in its Payments and Settlement Vision 2019-2021 (RBI (2019)).

91. In parallel, as payments are increasingly made remotely, fraud is shifting from the physical to the online environment. The market tries to counter this trend by developing fraud prevention and detection security tools with the objective of bringing online fraud rates down (eg implementation of 3D Secure, risk-based analysis, tokenisation or behavioural and/or biometric checks) and authorities try to steer this development by making certain security requirements mandatory (eg strong customer authentication in the European Union) (ECB (2018b)).

92. Another concern with electronic wallets and contactless technologies is interoperability (or the lack thereof). This is a common concern with new solutions that are, at least in the early stages of development, based on proprietary standards. If proprietary solutions gain a significant market share, thereby imposing de facto market standards, smaller providers may face challenges to gain traction and compete on a level playing field. With regard to contactless technologies, standardisation efforts have been made at both national and international level. In 2017, EMVCo published specifications for consumer-presented and merchant-presented QR codes. In some countries, authorities have taken on an active role in fostering interoperability of QR code payments. For instance, India has implemented a common QR code across all card networks called Bharat QR, and in the Philippines the central bank is working with the industry to develop a national standard. In the case of the Peruvian electronic wallet for e-money, Billetera Móvil (BiM), the lack of interoperability with deposit transaction accounts and the low coverage of agents, particularly in remote areas, are cited as factors limiting BiM's usefulness and uptake. In an effort to improve uptake, two banks enable cash-in through POS terminals; and interoperability between e-money and deposit transaction accounts via BiM is being discussed (Berkmen et al (2019)).

## 3.3 Awareness and financial literacy

### 3.3.1 End users' digital capabilities do not always keep pace with product evolution

93. According to the OECD (2018a), the growing digitalisation of daily life and of financial decisions is not necessarily matched by increasing digital (and financial) literacy levels, not even among the younger population. With the rapid digitalisation of payments digital capability (and access to digital technologies and the devices that support them; see Section 3.2.1) may become a precondition for navigating payment service offerings and for broader financial inclusion. This may make it more difficult for some groups less likely to be apt to use the latest technologies (eg the elderly) to be included in the first place, and may even drive those groups out of using financial services.[29]

[28] Bharat QR has been developed by NPCI, Visa and MasterCard, and has been adopted as the common QR Code across all card networks in India for person-to-merchant payments (NPCI (2020)).

[29] India's Electronic Banking Awareness and Training (e-BAAT) initiative, for example, tries to overcome these challenges. The e-BAAT programmes are conducted by RBI regional offices, focusing on financial literacy related to electronic payments, including their benefits and challenges (eg cyber security). Participants in these programmes are bank customers, students and the general public.

### 3.3.2 Big data analytics can break down knowledge barriers or reinforce exclusion patterns

94. Big data analytics tools such as AI and ML have the potential to increase users' awareness of the features of financial products as well as transmit tailored knowledge about their usage of financial products and management of financial resources. Increasingly, PSPs are utilising AI and ML for customer support (eg virtual assistants complementing telephone helpdesks), onboarding and customer education. This assistance can be integrated into an app and offer validation for crucial steps, thereby reducing the fear of making a mistake and losing money (Murthy et al (2019)). AI may also be used in the future to augment customers' ability to navigate information-dense product offerings. Savings products can incorporate robo-advice on how to allocate savings and set and meet savings targets, and thus nudge customers towards more sustainable financial practices. Text-to-speech applications can be used to help customers access and understand complex loan contract terms. In these examples, big data analytics could lift the financial education burden of educational and outreach programmes (FIBR (2018)).

95. Big data analytics, particularly when ML techniques are applied, require significant resources in order to be able to properly understand and maintain them. If not properly designed, maintained and controlled, big data analytics could have negative implications for unserved and underserved segments. For instance, when used to automate decision-making processes, big data analytics could reinforce existing biases against disadvantaged groups if checks are not put into place to evaluate the decisions of models with respect to their impact on those groups (FIBR (2018)). This can affect decisions about credit or insurance, and can lead to denied access to certain services or inappropriate charges based on inaccurate or wrong correlations made without human interpretation (OECD (2018a)). Furthermore, end users with higher risk profiles or a limited digital footprint might face increasing challenges to obtain financial access if the PSP relies heavily on big data analytics. Finally, big data analytics might result in a very granular marketing segmentation, limiting the choice of products and services offered to some end users (EBA-ESMA-EIOPA (2018), Bazarbash (2019)). Therefore, it is important to make sure that big data tools are designed in a way that fosters or at least is not detrimental to financial inclusion objectives, taking into consideration the challenges associated with a low level of financial literacy and cultural, gender-specific and/or religious factors.

Box K

## Principles for the use of big data analytics in the financial sector

The Netherlands Bank (DNB) suggests that principles are divided over six key aspects of responsible use of AI, namely: (i) soundness, (ii) accountability, (iii) fairness, (iv) ethics, (v) skills and (vi) transparency (or "SAFEST"). From a prudential perspective, soundness is the aspect of AI that is of primary concern to the DNB. AI applications in the financial sector should be reliable and accurate, behave predictably, and operate within the boundaries of applicable rules and regulations. This aspect becomes particularly important when financial firms start to apply identical (or relatively similar) AI-driven solutions and systemic risks might arise. Firms should also be accountable for their use of AI, as AI applications may not always function as intended and can result in damage to the firm itself, its customers and/or other relevant stakeholders. Although fairness is primarily a conduct risk issue, it is vital for society's trust in the financial sector that financial firms' AI applications – individually or collectively – do not inadvertently disadvantage certain groups of customers. Financial firms should therefore be able to define what their conception of fairness is and demonstrate how they ensure that their AI applications behave accordingly. As AI applications take on tasks that previously required human intelligence, ethics becomes increasingly important and financial firms should ensure that their customers, as well as other stakeholders, can trust that they are not mistreated or harmed – directly or indirectly – because of the firm's deployment of AI. When it comes to skills, from the work floor to the board room, people should have a sufficient understanding of the strengths and limitations of the AI-enabled systems they work with. Transparency, finally, means that financial firms should be able to explain how and why they use AI in their business processes and (where reasonably appropriate) how these applications function.

The European Banking Authority identifies eight elements of trust to be observed when rolling out big data analytics. These elements are: (i) ethics (AI solutions should adhere to some fundamental ethical principles, which can be embedded from the start in any AI); (ii) explainability and interpretability (the internal behaviour of a model can be directly understood by humans or explanations can be provided for the main factors that led to its output); (iii) fairness and avoidance of bias (the model ensures protection against direct and indirect discrimination); (iv) traceability and auditability (the model tracks all steps, criteria and choices throughout the process and is replicable); (v) data protection (the model's compliance with respective laws and regulations); (vi) data quality (throughout the lifecycle); (vii) security (ensuring that governance, oversight and the technical infrastructure are in place for effective ICT risk management); and (viii) consumer protection (with adequate redress procedures).

Sources: DNB (2019); EBA (2020).

## 3.4 Leveraging large-volume recurrent payment streams

### 3.4.1 Cross-border retail payments innovation can benefit from a mix of fintech developments

96. International remittances are ideally placed to foster access to, and use of, transaction accounts by both senders and recipients. However, this potential remains largely untapped due to remittance service users electing cash-based methods over transaction accounts. The higher costs associated with sending remittances through banks and with bank accounts have played a role in discouraging the channelling of remittances through transaction accounts. Therefore, transaction accounts that support international remittances at a low cost could make a significant contribution to financial inclusion.

97. The relative inefficiency and high costs of cross-border payments, such as international remittances, compared with domestic payments reflect in part the higher complexities and risks to be managed. Despite some promising developments in cross-border payments, improvements in the market for domestic retail payments have been more far-reaching (eg instant payments). Correspondent banking remains the prevalent back-end arrangement for cross-border retail payments. In this model, a series of correspondent banking relationships might be involved in a single payment transaction, thereby increasing

the complexity, cost and processing time of the transaction (CPMI (2018a)). Recent initiatives such as SWIFT gpi aim to reduce these frictions in the existing correspondent banking system.

98. Alternative solutions have emerged based on linkages between national payment infrastructures, the use of central platforms to connect domestic providers, or closed-loop models (where both payer and payee must subscribe to the same service). However, linkages between national payment infrastructures have not seen a large-scale deployment so far (World Bank (2014)), but may be revived in the future thanks to increasing standardisation and new political momentum.

99. Mobile money solutions have started to serve some international remittance corridors (GSMA (2018a)), initially through partnerships and recently through the development of payment hubs that connect service providers across countries. Closed-loop systems are considered to be the fastest-growing solution for cross-border payments (CPMI (2018a). Finally, new digital players aim to bypass correspondent banking relationships by eg using a network of local bank accounts and pairing transactions between different countries (eg Transferwise).

100. DLT may further spur business model innovation in cross-border payments. In a permissioned/private environment, DLT could support the streamlining of B2B cross-border payments (CPMI (2018a), Mejía-Ricart et al (2019)). Using DLT solutions could increase straight-through-processing rates, lower reconciliation costs, bring down compliance costs, and improve the transparency and traceability of transfers, thereby also easing the impact of de-risking issues.[30] Currently, such solutions are in the early stages of development or operating on a small scale. DLT could also support interoperability without requiring connections and institutional arrangements between ledgers. Recent research demonstrates the technical feasibility of synchronised settlement between different types of ledgers (including between DLT and centralised ledgers), thereby eliminating principal risk, with potential advantages for cross-border payments (ECB-BoJ (2019)). In a permissionless/public environment, remittance service providers (RSPs) seek to exploit the public blockchain to channel remittances. RSPs may use cryptoassets in the cross-currency leg, with neither the sender nor the beneficiary holding cryptoassets (B2B model) or provide cryptoassets wallets from which value is transferred directly from the sender's wallet to the recipient's wallet (P2P model), In the first model, the public blockchain essentially serves as the pipe for international transfers to alleviate complexities in the intermediate steps. However, this model leaves any challenges associated with the first and last mile unaddressed (eg CICO). Furthermore, the unregulated nature of some cryptoasset business may make it difficult to establish and maintain partnerships with local service providers (Parulava (2017)). The second model may expose users to cryptoasset risks. From an end user perspective, the usage of cryptoassets as a means to transact and store value has been starkly limited by their scarce acceptance, thereby subjecting their holders to "cashing out" costs, and by their sharp price fluctuations, potentially leading to substantial losses.

101. Recent global stablecoin initiatives purport to address shortcomings in cross-border payments by reducing the complexities and costs of (legacy) foreign exchange arrangements. Users of global stablecoins may send or receive stablecoins across country borders, without using transaction accounts (although they may be required to maintain a stablecoin wallet funded via a transaction account) or incurring FX fees. Resembling features of a closed-loop solution (see above), global stablecoin arrangements may enable faster cross-border remittances at potentially competitive costs. That said, depending on the stablecoin design and ecosystem, users (senders and receivers) may still need to exchange their holdings for sovereign currencies (and vice versa) to continue catering to the full range of their payment needs, and may bear additional costs (eg cash-out fees, idle balances) and risks (investment, credit, foreign exchange and custody risks). Furthermore, prices and service levels in the stablecoin

[30] The Financial Action Task Force (FATF) defines de-risking as "the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk […]. De-risking can be the result of various drivers, such as concerns about profitability, prudential requirements, anxiety after the global financial crisis, and reputational risk" (FATF (2014)).

arrangement's user interface may still reflect local market conditions in terms of competition and the availability of access points. Moreover, global stablecoin arrangements raise a host of concerns with regard to the safety and efficiency of the value transfer system as well as other public policy priorities, including AML/CFT, which lie beyond the scope of this report and are being dealt with by the relevant international forums.

### 3.4.2 Electronic wallets in combination with contactless technologies could support the efficient use of transaction accounts for transit payments

102. Where a significant share of a country's population, very often including economically disadvantaged individuals, uses public transit systems, the associated payment mechanisms offer the potential to reach the financially excluded. However, the PAFI report acknowledges that transit payments fall short of having a clear impact on financial inclusion because: (i) developing (electronic) transit fare schemes imposes a significant cost on the public transit operators; and (ii) most schemes are single-purpose and closed-loop, denying their users the benefits that a general-purpose electronic payment instrument would offer and preventing them from accessing their own funds for purposes other than transit payments. Yet the adoption of account-based and open-loop systems is not without complications, requiring transit companies to adhere to existing scheme rules and international standards and to pay merchant service charges to acquirers.

103. New technologies offer several options to facilitate the use of account-based, open-loop payment methods for public transit payments. NFC technologies are already being deployed successfully and support a variety of media – from payment cards to mobile phones and a variety of wearables. For instance, London's TfL has adopted an open-loop transit payment scheme accepting contactless cards and mobile wallets such as Apple Pay and Google Pay, which run parallel to the Oyster card's closed-loop system (TfL (2020)). Recently, the Shanghai Metro has adopted QR codes enabling its users to pay via Alipay or UnionPay. Biometrics (eg face recognition) are being tested, with China in the lead.

# 4. The role of the basic foundations in harnessing fintech's opportunities while addressing the challenges

104. The PAFI report identified three foundations as critical enablers of payment systems and the provision of payment services in general. These are: (i) public and private sector commitment; (ii) the legal and regulatory framework; and (iii) financial and ICT infrastructures. Building on Section 3, this section aims to determine how these foundations can cater to fintech-specific issues, with a view to, on the one hand, seizing fintech's opportunities (efficiency, market contestability, user experience and ubiquity) and, on the other, addressing the challenges (safety, market concentration, consumer protection and data privacy and digital exclusion).

## 4.1 Public and private sector commitment

### 4.1.1 Fintech developments call for increased international and cross-sectoral coordination between authorities

105. Having a well founded, clear, transparent and enforceable legal basis in all relevant jurisdictions is critical to the overall soundness of the payments system. Given that many technology-enabled products are offered across different jurisdictions, this could give rise to conflicts of law – eg in terms of AML/CFT, settlement finality, data localisation, data protection and/or consumer protection requirements. Furthermore, the fact that many providers operate at the crossroads of various fields (ICT, payments) makes the interaction between different authorities as necessary – eg in view of cooperative oversight arrangements – as it is complex (G7 (2019), (Taylor (2020)). Furthermore, to address challenges, customers might feel it is important that authorities understand and test fintech innovations in order to ensure that consumer protection and other legal and regulatory frameworks address potential risks[31] (GPFI (2016)), OECD (2018b)).

106. The increasing array of new products, often offered by new entrants and/or without in-person end user support, might make it difficult for end users to establish the necessary trust to adopt financial services. Especially underserved and unserved groups might feel more confident if a sound framework is in place that protects consumers, their data and funds, and is able to cope with fintech developments. In view of the increasing volume, variety and velocity of the personal data being used and processed, it is important that consumer protection frameworks be closely aligned with data protection frameworks (Section 4.2.2).

[31] For concrete country approaches to financial consumer protection in the digital environment, see OECD (2018b).

Box L

## Examples of domestic and international coordination on fintech between authorities in Latin America and the Caribbean

Mexico's Law to Regulate Financial Technology Institutions calls for the establishment of a Financial Innovation Group, which is a consultative and coordination body comprised of representatives from the Ministry of Finance and Public Credit, each Supervisory Commission and the Bank of Mexico as well as representatives of the private sector. This body will aim to provide an instance through which its members can share knowledge about fintech innovations in order to plan its orderly development and regulation.

A regional example of authorities' coordination is CEMLA's Forum of FINTECH Experts, also known as the Fintech Forum, for countries in Latin America and the Caribbean. The goal is to bring together the knowledge and experience of central banks in the region, international organisations and other relevant institutions to analyse the dimensions and potential impact of the fintech phenomenon in central banking mandates.

Sources: BBVA (2018); CEMLA (2020).

107. The need for international and cross-sectoral coordination between authorities has become more urgent in the wake of global stablecoin initiatives. Following the announcement of Libra, a G7 working group, consisting of senior officials from the G7 central banks and ministries of finance as well as the IMF, the BIS and the Financial Stability Board (FSB), supported by the CPMI, was convened to analyse stablecoins and put forward key considerations as a baseline for critical issues to be solved (G7 (2019)). The group emphasised the need for a globally coordinated and consistent response to mitigate the risk of cross-border regulatory arbitrage and recommended that authorities improve coordination, including through strong regulatory cooperation and harmonised standards, where practicable, and by establishing information-sharing and cooperative oversight arrangements. At the time of writing, the FSB is looking into the regulatory issues of stablecoins and will submit a report to the G20 in the course of 2020 (FSB (2019b)).

108. To foster international collaboration on fintech developments within the central bank community, complementing the already well established cooperation within the existing standard-setting bodies (SSBs), the BIS set up an Innovation Hub in 2019. The role of the Hub is to identify and develop in-depth insights into critical trends in technology affecting central banking; develop public goods in the technology space geared towards improving the functioning of the global financial system; and serve as a focal point for a network of central bank experts on innovation (BIS (2020a)). Furthermore, in 2020 the BIS and a group of six central banks[32] created a group to share experiences to assess the potential cases for CBDC in their home jurisdictions (BIS (2020b)).

### 4.1.2 A collaborative approach to fintech is key to making an impact

109. There is a growing trend towards collaboration between fintech startups and traditional financial institutions. This collaboration can be mutually beneficial: fintech startups gain access to new markets and capital, whereas the traditional providers develop innovative capabilities and competitive advantage over their peers (Deloitte (2017)). Besides traditional mergers/acquisitions and venture capital, this collaboration between private sector stakeholders can take the form of incubators, accelerators, innovation labs and industry-led sandboxes. Incubators help early-stage startups hone and refine ideas and business models, and move them towards market deployment. Accelerators generally work with more mature concepts and startups, contributing some seed investment and other support to accelerate growth and advance maturity. Innovation labs are generally collaborative and cooperative communities that foster

[32] The Bank of Canada, the ECB, the Bank of Japan, Sveriges Riksbank, the Swiss National Bank and the Bank of England.

building capacity, increased creativity and growth, and can sometimes comprise public-private partnerships. Industry-led sandboxes provide an environment for "off-market" testing and experimentation, as well as a development environment, with tools, shared data, APIs, sandbox-as-a-service and collaborative platforms (BCBS (2018), Wechsler et al (2018)).

110. Smaller countries can benefit from a coordinated approach to fintech to overcome capacity and scalability constraints. For instance, the ASEAN Financial Innovation Network (AFIN)[33] launched with API Exchange (APIX) a cross-border marketplace and sandbox environment to facilitate the adoption of APIs to drive financial inclusion across the Asia-Pacific region (UNSGSA (2019), Davidović et al (2019)).

### 4.1.3 Regulators' initiatives such as sandboxes, innovation hubs and innovation offices can foster the development of the fintech ecosystem

111. A so-called regulatory sandbox is generally a regulator-controlled environment that allows private sector participants to test their products and services prior to formal licensing or registration. Alternatively, regulatory sandboxes can be used to evaluate regulations or policies that may impede beneficial new technologies or business models (UNSGSA (2019)). A sandbox differs from regulatory tools (Section 4) insofar it is a flexible exercise at the regulator's discretion, normally within the parameters of the existing legal and regulatory framework (Cenfri (2019)). Thematic sandboxes, such as those introduced by the Bank of Thailand (QR code standard), RBI (payment system development facilitation) and the Japan Financial Services Agency (KYC-related technology), can focus on fintech developments that support payment aspects of financial inclusion (UNSGSA (2019)). The 2019 CGAP-World Bank Regulatory Sandbox Global Survey shows that 21 sandboxes worldwide (out of 23 in the sample) are sponsored by authorities/agencies with a financial inclusion mandate, and in the majority of cases payments are the most common sector represented by participating providers (Appaya and Jenik (2019)).

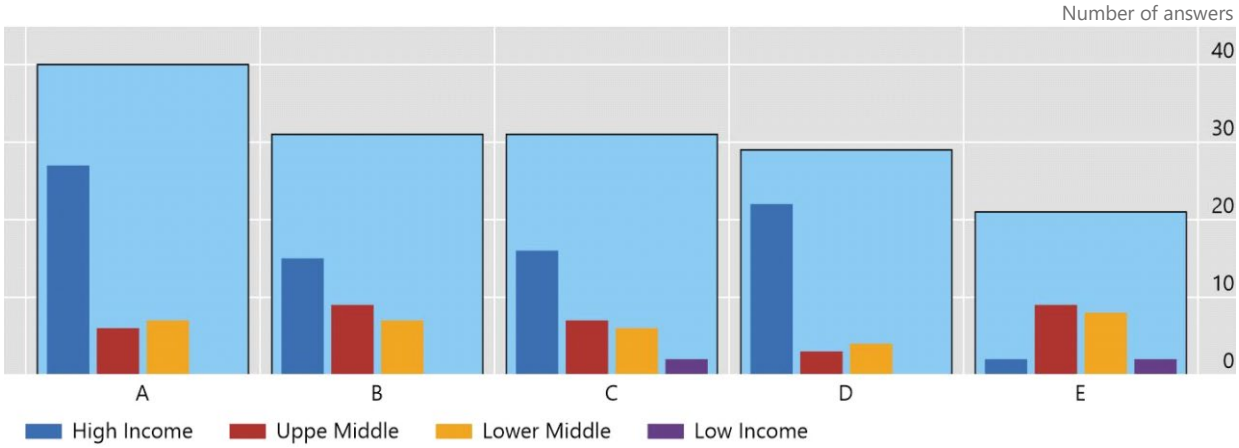
112. The term "innovation hub" generally refers to a regulator-provided knowledge centre open to regulated and unregulated entities. This approach has become a popular complement to the regulatory sandbox. Its form and breadth of offerings can vary.[34] Innovators receive guidance, advice and assistance from hub staff or third-party experts regarding matters such as licensing issues and navigating complex legal and regulatory systems. The hub can also serve as an opportunity for regulators to learn more about the industry through direct interaction (BCBS (2018), Wechsler et al (2018)).

113. Innovation offices are structures held by the regulator to provide regulatory clarification to financial service providers that seek to offer innovative products and services, and can be considered as a first step towards obtaining regulatory approval. The key objective of innovation offices is to facilitate regulator-innovator engagement and mutual learning in a pro-innovation setting. This interaction helps regulators identify emerging issues and may inform policy developments. It is also essential for innovators, as it helps them understand the current regulatory landscape in a local context and where fintech-related regulations may be heading. This approach is very often a compelling option for capacity-constrained regulators in EMDEs (UNSGSA (2019)).

[33] AFIN was established as a non-profit organisation in 2018 by the ASEAN Bankers Association (ABA), the International Finance Corporation (IFC) and the Monetary Authority of Singapore (MAS). AMTD Foundation and Mastercard are AFIN's Corporate Founding Members (APIX (2020)).

[34] In India, a payment and settlement systems innovation contest was recently conducted by the RBI to provide a platform to encourage, recognise and promote innovations and ideas in the payment and settlement systems arena as well as foster new developments by entrepreneurs, start-ups and similar entities in the payments space.

Authorities' approaches to facilitate the development of Fintech Graph 2




A = "Set up special contact point for fintech"; B = "Allowed sandboxes"; C = "Other [Please provide brief description]"; D = "Established Innovation hubs"; E = "None".

Source: IMF-World Bank (2019).

114. The experience so far shows that these initiatives, while contributing to the development of the fintech ecosystem, are neither necessary nor sufficient to increase access to and usage of transaction accounts. However, authorities can try to foster financial inclusion with a targeted approach, by making financial inclusion aspects an integral part of regulatory sandboxes, innovation hubs and innovation offices. This could materialise in eligibility criteria for access to a regulatory sandbox that include the requirement that the fintech product or business model targets unserved or underserved customers, the inclusion of these customers in the testing samples and/or special treatment of providers which are deemed to be most relevant for financial inclusion. Authorities would need to put appropriate safeguards in place, though, to ensure the protection of more vulnerable customers and that providers live up to their commitment.

115. Sandboxes and other regulators' initiatives covered in this section are not necessarily suitable for every jurisdiction. Many of these approaches are resource-intensive and require careful cost-benefit analysis. The decision on the approach chosen should be influenced by the authority's mandate (determining its ability to implement the initiative, and the flexibility and the utility of the approach chosen), the stakeholder ecosystem (which might require the involvement of more than one authority), the availability of adequate capacity and resources, existing market conditions and policy priorities (Jenik and Lauer (2017), UNSGSA (2019)). In any event, a sandbox or similar approach should not prevent authorities from reviewing the legal and regulatory framework with a view to ensuring that it keeps pace with fintech developments (Section 4.2).

116. The government can also support the growth of fintech developments through policies and programmes (eg tax exemptions, patent reforms) and by providing funding. Such policies and programmes can target fintech developments directly (eg tax exemptions or patent reforms tailored to fintech innovations) or create environmental conditions conducive to fintech developments, by trying to steer the use of electronic payment instruments (Box M).

Box M

### Government policies fostering adoption of electronic payments

While in Japan contactless transit payments and mobile payments were already launched in the early 2000s, cash is still by far the preferred payment instrument. The Japanese government announced in 2018 that it aims to bring its cashless payments ratio for consumer payments up to 40% by 2025 (from 20% in 2018). As a supporting measure, customers opting for non-cash payments in SMEs are able to receive reward points to offset the consumption tax increase introduced in 2019. This measure triggered a strong response from SMEs: 940,000 stores registered between May and December 2019 for the scheme, many of them not having offered electronic payments before (Lewis (2019)).

In India, following the demonetisation of its INR 500 and INR 1,000 notes in November 2016, the government announced several measures to increase the pace of digitalisation. It reduced the maximum value allowed for cash transactions, lowered permissible cash donations to political parties, and announced various incentives for making electronic payments, such as a service tax waiver for certain amounts of digital payments. In addition, it waived transaction charges for digital payments made to government agencies and offered discounts and rewards for making digital payments. The Reserve Bank of India also relaxed customer charges for various electronic payment methods (Roy and Rai (2017)). Effective January 2020, the merchant service charge on RuPay debit card transactions and UPI transactions have been set at zero by the Indian government.

## 4.2 Legal and regulatory framework

### 4.2.1 Adapted and new licensing frameworks enable new players to leverage fintech for innovative services

117. Several jurisdictions around the world have recognised the emergence of technology-enabled business models in payments and other financial services, and introduced reforms to foster these developments. Regulators have established tiers within existing licence categories or have drawn up new licensing frameworks that enable new players to leverage fintech developments to provide innovative services. Another way to add flexibility to licensing regimes is by phasing in existing requirements for new entrants until they fully apply or customise requirements based on the combination of activities performed by each bank to reflect their different risk levels (Dias (2020)). Stated objectives of these efforts are enhanced innovation, competition and/or financial inclusion (Box N).

Box N

## Examples of new licensing frameworks for innovative business models

The European Commission proposed to review the Payment Services Directive (PSD) with a view to modernising it to take account of new types of payment services, such as payment initiation services. These service providers had the potential to introduce innovation and competition – eg by providing more, and often cheaper, alternatives for internet payments – but they were previously unregulated. By bringing them within the scope of the PSD, the European Commission aimed to increase transparency, innovation and security in the European single market and enhance the level playing field between different PSPs. The Second Payment Services Directive (PSD2), which entered into force in January 2016 with rules applying as from January 2018, created two new types of PSP: account information service providers (AISPs) and payment initiation service providers (PISPs). Both AISPs and PISPs are licensed third-party providers (TPPs) in the framework of PSD2. PSD2 further prescribes that AISPs and PISPs provide TPPs free access to payment account information via open APIs.

In 2013, India's Committee on Comprehensive Financial Services for Small Businesses and Low Income Households recommended the concept of differentiated banks to further the cause of financial inclusion and deepening of strategies, using the functional building blocks of payments, deposits and credits. Specifically, the Committee recommended the licensing of payments banks, whose primary role would be to provide payment services and deposit products to small businesses and low-income households. Pursuant to the recommendations of the Committee and the subsequent announcement made in the Union Budget 2014-2015, Guidelines for Licensing of Payments Banks were issued by the Reserve Bank of India (RBI) in November 2017, based on the discussions with the government and the comments received from the public. The primary objective of setting up payments banks is to further financial inclusion by providing (i) small savings accounts and (ii) payments/remittance services to the migrant labour workforce, low-income households, small businesses, other unorganised sector entities and other users by enabling high-volume, low-value transactions in deposits and payments/remittance services in a secured technology-driven environment. The RBI currently lists seven active payments banks.

In Mexico, the Law to Regulate Financial Technology Institutions was enacted in March 2018. The Law has common elements with prudential regulation, as it seeks to protect consumers, prevent potential financial stability risks and reduce existing barriers to innovation. The Law was drafted in principle-based terms taking into consideration the dynamic nature of the industry and leaving room for the development of secondary rules with specific details. The principles of the Mexican Fintech Law are the following: (i) financial inclusion and financial innovation; (ii) fostering of financial competition; (iii) consumer protection; (iv) financial stability; (v) prevention of illegal activities (AML/ CFT); and (vi) technology neutrality. The Law regulates the organisation, operation, functioning and authorisation of institutions that offer financial services and products through alternative channels such as the internet, computer applications, interfaces or any other electronic or digital communications and alternative business schemes. For legal purposes, such institutions are defined as Financial Technology Institutions (FTIs) and are classified according to their core business activities, namely as (i) collective financing institutions or (ii) electronic payment institutions. A key element of this legislation is the creation of the Mexican Regulatory Sandbox, whose main purpose is to test innovative models in a controlled scenario. Regulated financial institutions or companies with innovative models require a temporary authorisation to engage in regulated activities under close surveillance and communication with authorities. The Mexican Fintech Law also requires that financial institutions (including FTIs) develop APIs to share their financial, aggregate and transactional data (with the prior consent of users). For cryptoassets, the Law recognises as such those that are determined by the Bank of Mexico through secondary rules and entrusts to the central bank the authorisation of operations based on such assets under terms and conditions which it may determine in such rules. Finally, in the last quarter of 2018, a secondary regulation regarding FTIs was published which establishes provisions regarding information disclosure, capital requirements, accounting criteria and client profile risk methodologies, among others.

To promote innovation in financial services and remove barriers to market entry for new players, the Swiss parliament has introduced a fintech licence. Since 1 January 2019, companies that operate beyond the core activities characteristic of banks have been able to accept public funds of up to a maximum of CHF 100 million on a professional basis subject to simplified requirements. These fintechs, however, are not allowed to invest the funds or pay interest on them. The Swiss financial market supervisory authority (FINMA) is the authority that licenses and supervises fintech companies. When Indonesia's first mobile money platform, TCash, was launched in 2007, the initial business model deployed via the mobile network operator struggled due to a restrictive public policy that resulted in the lack of an active agent network for cash-out services. As policies changed and the country's financial inclusion programme developed further, utilisation of the digital payment ecosystem eventually grew as expected. Recently, the Indonesian state-owned mobile payment platform launched the LinkAja application, which integrates the four state-owned banks, the national telecoms company, including TCash, and the state-owned energy corporation to further facilitate digital payments, financial services and funds transfers. Ongoing public-private partnerships are developing to enable banks to provide better services to the public and satisfy the market demand for QR code payments.

Sources: Reserve Bank of India (2020); CEMLA (2019).

118. In some jurisdictions (eg Hong Kong, Korea and Singapore), business model innovation in banking has led regulators to design a special licensing regime for "digital banks" or "virtual banks". Sometimes referred to as challenger banks, which tend to be established, mid-size or specialist firms seeking to compete with larger institutions, or neobanks, which are typically new entrants basing their service solely on digital and mobile channels, these business models have in common the prominent use of new technologies, leaner organisational structures and smaller branch bases or no physical presence at all (European Parliament (2018)).

119. Virtual banks try to differentiate themselves in terms of customer experience and pricing, and often focus on payment and savings products first. Easy customer onboarding processes, simple and low fee-charging models, and customer-centric design are all features that can catalyse access to and usage of transaction accounts; some virtual banks even target financially excluded persons (Noonan (2019)). Many virtual banks have already successfully expanded to third-country markets and/or are including international remittances in their service offering. While many virtual banks have been established in markets that already have relatively high financial inclusion figures and often serve as a second or third banking relationship rather than the primary account for their customers, in over 20 EMDEs a total of 35 virtual banks are offering their services (Jenik and Zetterli (2020)). Prominent examples of virtual banks exist in Brazil (eg Nubank), China (MyBank, AiBank and WeBank), Germany (eg N26), the United Kingdom (eg Revolut, Monzo) and the United States (eg Chime).

### 4.2.2 Data frameworks need to ensure privacy in the fintech era

120. While the increased availability and flow of personal data may be beneficial for financial inclusion, it also poses new risks for individuals (Section 3.1.2). Missing or uninformed consent to the use and/or sharing of personal information, illegal discrimination, unfair price segmentation and data privacy are key concerns for policymakers. Moreover, the repercussions of data security issues increase along with the amount of personal information stored and shared in digital form.

121. Authorities may need to update existing national data frameworks to clarify the rights and obligations of key stakeholders. These include: (i) data subjects (who the data are about); (ii) public authorities (who enact and enforce laws); (iii) controllers (who have an interest in using the data); and (iv) processors (who would collect, store, transfer and analyse the data on behalf of the controllers). Innovative legal frameworks, such as the 2018 General Data Protection Regulation in the European Union, India's 2018 Personal Data Protection Bill and Australia's 2019 Consumer Data Right Act, clarify the rights and obligations of these stakeholders while introducing important principles that have a bearing on the use and sharing of personal data such as data minimisation, informed consent and data portability, among others (Grady et al (2018)).

122. Where a provider permits access to or transfer of personal data (for legitimate business purposes) to third parties, it should take steps to ensure that the data remain protected. First, providers should set minimum default policies for sharing personal information that may pose risks to customers. Second, they should draw up written agreements with third parties (either processing personal data or having access to personal data) to determine responsibilities for data privacy (GSMA (2018c)).

### 4.2.3 Fintech developments may challenge the applicability of current oversight concepts and standards

123. A level playing field between traditional payment infrastructures and new arrangements needs to be ensured. As most oversight standards and payment regulations predate recent fintech developments, it is important to ensure that requirements do not discriminate against the use of a particular technology or disregard new technologies altogether. Ideally, requirements are technology-neutral; nonetheless, they should be assessed periodically to ensure that they are future-proof to the extent possible. Regarding DLT specifically, the CPMI concluded that the requirements as set by the CPMI-IOSCO *Principles for financial market infrastructures* (PFMI) are of a sufficiently high level to accommodate the use of DLT, to the extent the system has an identifiable responsible operator (CPMI (2017)).

124. Increased specialisation and distributed setups raise questions around governance. Clear lines of responsibility are an essential component to ensure the overall safety and integrity of a payment infrastructure and/or arrangement. The involvement of a large number of specialised providers could hamper the decision-making pertaining to the payment infrastructure's or arrangement's design and technological evolution or by slowing incident responses related to operational issues. Where the operator or PSP relies on intermediaries and/or outsourcing to third-party service providers, it should be in a position to review and control the risks it bears from and poses to other entities to the same extent that it would for the services it operates itself. Annex F of the PFMI, outlining five oversight expectations for critical service providers in order to support a financial market infrastructure's (FMI's) overall safety and efficiency, can be a minimum requirement to cater for this. A related question is the possible oversight and/or supervision of third-party service providers themselves, which in many cases may not be in the remit of the central bank and may require collaboration with other authorities.

### 4.2.4 Fintech developments should not compromise the effective protection of end user funds

125. The PAFI report emphasises the importance of protecting customer funds against misuse and loss, irrespective of whether they are held in deposit or e-money transaction accounts. In particular, the report underlines the importance of protecting customer funds through appropriate design and risk management measures such as deposit insurance or functionally equivalent mechanisms, as well as through preventive measures (eg supervision, placement of customer funds held by non-deposit-taking PSPs in high-quality and liquid assets, and, depending on the legal regime, specially protected accounts at banks such as escrow accounts and possibly trust accounts). The report goes on to mention the most common set of risk mitigation measures that regulators have adopted and elaborates on specific country examples. Since then, some more countries have implemented measures to protect customer funds in e-money transaction accounts, or are in the process of doing so (Izaguirre et al (2019)).

126. Just as with deposit accounts, e-money account holders are subject to the risk of the e-money issuer going into bankruptcy, which could result in the illiquidity or loss of the customer funds it manages. While this risk could be mitigated through deposit insurance, which is directly beneficial to the customer, most financial authorities around the world have adopted other approaches. With these measures, however, holders of e-money accounts can become exposed to a new risk in addition to the risk of the bankruptcy of the e-money issuer itself, which is the risk of the bankruptcy of the deposit-taking institution that holds the trust account with the e-money float. For instance, if the deposit liability of the deposit-taking institution holding the trust account is only to the e-money issuer and not to the e-money account

holder, the latter may not have ready access to its funds in either the deposit-taking institution's insolvency or the e-money issuer's insolvency. Thus a safe regime will need to consider both the bankruptcy of the e-money issuer and the bankruptcy of the deposit-taking institution holding the trust account as dual risks to the customer, and to design appropriate funds segregation and customer protection.

127. Achieving appropriate protection may be particularly challenging in the context of cryptoassets and stablecoins. In the absence of adequate regulation and supervision, users' holdings of cryptoassets do not benefit from the legal protection associated with regulated instruments. For instance, in the event of bankruptcy or hacking of a cryptoasset service provider that controls access to customers' holdings of cryptoassets (eg custodian wallet providers), the holdings would neither be subject to preventive measures (eg safeguarding and segregation) nor benefit from schemes or other arrangements to cover any losses incurred (Chimienti et al (2019)).

128. Issuers of stablecoins may also misuse reserve funds and/or assets (eg lack of segregation of assets) and may be unable to honour redemptions as advertised, and hence shall be subject to regulation, oversight and supervision. Credit and liquidity risks of the underlying bank and/or issuer of reserve assets may also lead to the stablecoin issuer being unable to meet redemption requests (G7 (2019), Cuervo et al (2020)). In fact, not all stablecoin issuers may commit to redeeming users' holdings, or redemption pledges may vary (face value vs market value of the underlying assets). Furthermore, stablecoin designs differ markedly according to the nature of the claim users have, and the type of assets used. In view of the novelty of stablecoins and the ongoing work on regulatory and supervisory approaches, measures for the protection of customer funds are in most cases yet to be implemented (G7 (2019)).

### 4.2.5 Regulatory technologies can support authorities in fulfilling their supervisory and oversight tasks and market participants in meeting requirements more effectively and efficiently

129. Regulatory technology (regtech) focuses on the use of fintech innovations to solve regulatory, oversight and compliance requirements more effectively and efficiently, including but not limited to the challenges introduced by fintech developments. As such, regtech can be defined as a subset of fintech and can be further differentiated into regtech for financial institutions and regtech for authorities. Regtech heavily relies on big data analytics and supporting fintech technologies, such as APIs, cloud computing and DLT, and combines them with innovative processes to modernise the way supervisory and oversight data are gathered, organised and analysed (Toronto Centre (2018), UNSGSA (2019)).

130. Regtech can enable market participants to improve risk management and stay abreast of changing regulatory and oversight requirements while reducing compliance costs. Discussions on regtech often focus on regulatory reporting, by helping to automate and integrate regulatory reporting requirements, reducing the need for manual intervention, and increasing accuracy and timeliness (up to real-time reporting). Another important area of regtech is compliance, including solutions for automated identification of new or changing regulatory requirements, the embedding of these requirements into algorithms, and the monitoring of compliance risk and compliance levels. Customer due diligence and AML/CFT controls are another field where regtech holds significant promise in terms of reducing false positives and resulting manual interventions. Regtech solutions based on transaction monitoring and auditing can support AML/CFT compliance and fraud detection, and provide tools to improve overall risk management (Toronto Centre (2018), UNSGSA (2019)).

131. An increasing number of authorities have or are in the process of developing explicit strategies to leverage regtech for their purposes (often referred to as "regtech for authorities" or "suptech"). A recent analysis by the Financial Stability Institute (FSI) among 39 financial authorities from 31 jurisdictions found that about half of them have or are working on a specific suptech roadmap and/or digital transformation programmes (Ehrentraud et al (2020), di Castri et al (2019)). Many authorities have already implemented bespoke regtech solutions to support their tasks, especially for collecting data (including automated

reporting in market participant push and/or authority pull mode; real-time monitoring; data management, including data validation and consolidation; and virtual assistance by means of chatbots and machine-readable regulations) and analysing data (for market surveillance, misconduct analysis (especially for AML/CFT purposes – see Section 4.2.6 – and fraud detection), microprudential supervision and macroprudential supervision) (Broeders and Prenio (2018), di Castri et al (2019)).

132. Improvements in the efficiency and efficacy of compliance and supervision based on regtech might also support financial inclusion efforts. Regtech solutions improving reporting processes are already being used in the context of financial inclusion by several central banks, especially in EMDEs (Box O). For instance, the amount of transactional and non-transactional data that market participants are generating is constantly increasing, and market participants and authorities are devoting substantial resources to ensuring compliance (eg with AML/CFT requirements). However, many authorities face capacity constraints, particularly those in EMDEs. Suptech solutions, especially those based on big data analytics, can help authorities save time, allowing them to dedicate more staff resources for judgment-based work, rather than manual work (Coelho et al (2019)).

133. At the same time, as big data analytics require high computational capacity, a decision to implement any such solution needs to consider the necessary IT resources in-house or externally (eg via cloud computing). When relying on external partners in developing and/or operating the suptech solution, authorities need to be conscious of data privacy and confidentiality requirements. Suptech tools based on ML might require retraining from time to time in order not to lose their effectiveness in view of the changing behaviour of criminals (Coelho et al (2019)).

Box O

## Central banks using regtech for financial inclusion

The National Bank of Rwanda (BNR) has introduced an electronic data warehouse (EDW) system to automate and streamline the reporting processes that inform and facilitate supervision. The EDW allows the BNR to automatically "pull" data, from the reporting agents' systems, and to collect gender-disaggregated data on the uptake and usage of transaction accounts and other financial services.

The Central Bank of Nigeria and the Nigeria Inter-Bank Settlement System are developing a "data stack" that would include a data warehouse and dashboards; allow risk-based and timely financial supervision; and inform new strategies such as financial inclusion policies and regulatory interventions.

The Central Bank of Brazil has implemented a web-based compliance and information system for small supervised entities.

The Central Bank of Nepal has launched a financial inclusion portal to track financial inclusion progress based on real-time data reporting. Financial institutions can upload data via a smartphone app developed for the purpose of collecting data on access points along with geospatial information. The analysis of the data helps the central bank prioritise the approval of bank branches and determine the number of agents needed. Real-time data reporting might also allow authorities to introduce tiered KYC requirements, since they can be more suitable to detecting possible circumvention attempts based on real-time big data analytics, such as transaction splitting and/or opening of multiple accounts

Sources: World Bank (2017); di Castri et al (2018); Gurung and Perlman (2018); Sy et al (2019).

## 4.3 Financial and ICT infrastructures

### 4.3.1 Fintech developments highlight the opportunities and challenges of non-bank access to payment infrastructures

134. The PAFI report noted that restricting access of new entrants to financial and ICT infrastructures tends to constrain the supply of payment services to users. Meanwhile, the role of new providers in retail payment services, driving innovation forward and addressing emerging and/or unattended needs, has expanded significantly. As these providers grow, they may want to reduce their reliance on banks, with which they compete, to access clearing and settlement services (BoE (2016)). Therefore, while non-bank access to payment systems is not strictly a fintech-related issue, it has become a more pressing issue in light of fintech developments.

135. While many jurisdictions have introduced the possibility for authorised/regulated non-banks to offer payment services to end users, the access to payment infrastructures for clearing and settlement of transactions in many countries still requires a banking licence (Box P). Often incumbents with a dominant position in one infrastructure have an incentive to create barriers for access to new entrants.

136. Without direct participation in payment infrastructures, non-banks have only indirect access, potentially raising level playing field concerns. If given direct access to payment infrastructures, non-banks can compete on equal terms with banks. However, there are some more fundamental challenges to accessing the messaging, clearing and settlement service infrastructures, including those associated with technical, legal/regulatory and financial viability issues (ie direct access might be too expensive). On the other hand, non-banks should not increase the risk profile of the financial infrastructures in which they are a participant. Following a functional approach, non-banks are expected to meet the same criteria and abide by the same requirements as a traditional PSP – that is, the same activities and the same risks should face the same regulations and oversight. This is in line with the original PAFI guidance[35] and has been emphasised again in view of recent fintech developments (Khiaonarong and Goh (2020), G7 (2019)).

137. International standards support, under certain conditions, the participation of authorised non-bank PSPs in financial market infrastructures. Specifically, Principle 18 of the PFMI requires FMI operators to set participation requirements that have the least restrictive impact on access that circumstances permit. Any such restrictions should be justified in terms of the safety and efficiency of the FMI and the market it serves and be tailored to and commensurate with the FMI's specific risks. Operators and authorities should assess based on actual risks whether non-banks can be given access to their system within the existing legal and regulatory framework. In addition to legal risk, other risks (such as credit, liquidity and operational risk) would need to be assessed to ensure that non-bank participants do not increase risk levels.

138. Even if direct access was in principle allowed by the payment infrastructure rules, for non-bank PSPs gaining direct access might still not be feasible or desirable. Effective access to payment infrastructures may not be feasible if there are barriers to accessing the telecommunications networks serving those infrastructures or if investments, in order to fulfil the infrastructure's access criteria, are considered too high. Other than one-off investments, the operational costs of a direct participation might be considered too high by non-bank PSPs (eg in terms of the number of operational staff needed to manage direct participation, possible extension of business hours and/or a payment infrastructure pricing model geared towards large transaction volumes). In such cases, non-bank PSPs might still need to revert to indirect access mechanisms (ITU-T Focus Group Digital Financial Services (2016)).

[35] One of the key considerations of action in the PAFI report highlights the importance of the legal and regulatory framework promoting competition in the marketplace by providing clarity on the criteria that must be met to offer specific types of service, and by setting functional requirements that are applied consistently to all PSPs.

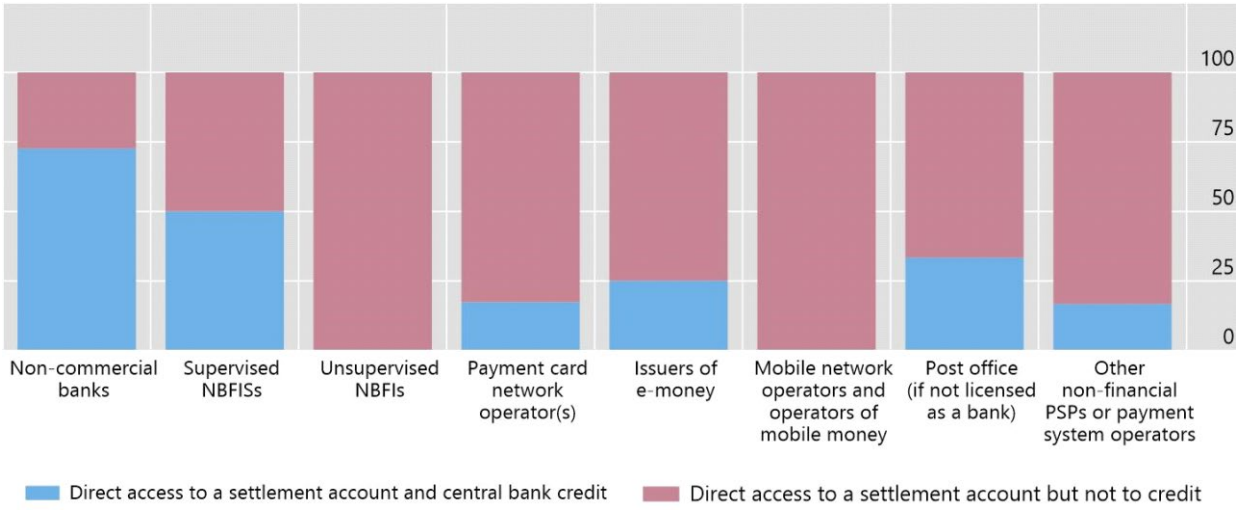
Box P

## Non-bank access to core payment infrastructures: country experiences

In recent years, several central banks have enabled regulated/authorised non-bank PSPs to access their RTGS systems, or at least announced their intention to do so. Based on the World Bank's Global Payment Systems Survey 2019, in more than 30 countries supervised non-bank financial institutions (NBFIs) have direct access to a RTGS settlement account (with or without central bank credit), and more countries are considering giving access to non-bank PSPs specifically.

### Access to RTGS systems

Graph P




Source: World Bank (2019d).

In 2017, the Bank of England extended access to its RTGS system to non-bank PSPs for settlement account purposes. This change enabled non-bank PSPs to directly access for the first time the UK payment schemes that settle in central bank money, including Faster Payments (BoE (2018)). Since 2014, the Faster Payments Access Programme has more than tripled direct participation in the scheme.

In January 2019, the Swiss National Bank (SNB) made a decision to grant entities with a fintech licence access to the Swiss Interbank Clearing (SIC) system and to sight deposit accounts, provided their business model qualifies them as "significant participants" in the area of Swiss franc payment transactions. Applicants need to make a significant contribution to the fulfilment of the SNB's statutory tasks of ensuring and facilitating the functioning of cashless payment systems, and their admission must not pose any major risks.

In June 2019, the Reserve Bank of Australia (RBA) issued recommendations for the New Payments Platform (NPP), the Australian instant payment system developed by a consortium of 13 financial institutions and launched in February 2018. The recommendation are based on the conclusions from a public consultation on NPP access and functionality that the RBA had undertaken with input and assistance from the Australian Competition and Consumer Commission (ACCC). As regards direct access, it was recommended that it should be open to a range of payment service providers and NPP Australia Limited should assess options for amending the NPP Regulations, and other arrangements, to allow for an entity that is not an authorised deposit-taking institution to potentially become an NPP participant. The participation of non-banks would be subject to requirements appropriately tailored and calibrated to the key risk and operational considerations essential for participation in the NPP (RBA (2019)).

The Reserve Bank of India (RBI) will review the membership of centralised payment systems as part of its Payments and Settlement Vision 2019-2021. The RBI has already permitted participation of non-banks in certain payment infrastructure and will initiate discussion to develop a framework for settlement risk management with increased participation of non-banks (RBI (2019)).

139. The emergence of Payments-Platform-as-a-Service – cloud-based platforms that provide on-demand access to a range of payment processing services – may enable cost reductions by allowing financial institutions to outsource their connection to clearing and settlement infrastructures via a single platform. At the same time, as the market for cloud computing is dominated by a few large companies, outsourcing to cloud service providers may raise challenges with regard to concentration risk (EBA (2017)). The risk is relevant not only from the point of view of individual institutions but also at industry level, as large suppliers of cloud services can become a single point of failure when many institutions rely on them. Still, lock-in risk is not specific to cloud computing and can be mitigated through effective approaches to outsourcing.

140. In addition to access to payment infrastructures, the question of non-banks opening central bank accounts is re-emerging in the context of fintech. Some central banks, such as the Hong Kong Monetary Authority, the Reserve Bank of India and the Swiss National Bank already offer special purpose licences that allow non-bank fintech firms to hold reserve balances, subject to an approval process.[36] In addition to banks, some non-bank electronic wallet operators in Hong Kong SAR have been granted access to the HKMA's instant payment system, FPS. The Bank of England is discussing such prospects. Meanwhile, China has gone even further: the People's Bank requires the country's large payment providers, Alipay and WeChat Pay, to hold client funds at the central bank in the form of reserves (Adrian and Mancini Griffoli (2019)).

### 4.3.2 Fintech goes hand in hand with raising the bar for the cyber resilience of PSPs and financial infrastructures

141. Cyber risks are a corollary of digitalisation and a permanent risk feature of digital services. The financial market in particular is a very prominent target due to its interdependencies, its assets and its systemic implications for the real economy. Although cyber risks are not unique to fintech developments, increased connectivity and new entrants increase the entry points for cyber criminals and the potential for successful attacks (Lukonga (2018)). The outsourcing to third parties can exacerbate the risk by further expanding the surface of attack and the attractiveness to malicious actors. This might especially be true in a DLT setup with many parties involved and/or with big cloud computing providers concentrating the business of many market participants.

142. Cyber security risks (once they materialise) can be especially damaging for the inexperienced end users in their first encounters with financial services and have the potential to undermine their trust in financial services altogether, thus deterring financial inclusion. Furthermore, low-income customers are the least able to rebound from an incident resulting in financial losses (CGAP (2018)). Cyber attackers are targeting markets and/or stakeholders which tend to have weaker cyber resilience in place, on both the demand (users) and the supply side of the market (financial service providers). In the case of less experienced entities, not only the detection, protection and recovery capabilities may be weaker, but also the communication and redress strategies could be insufficient to respond to a large-scale attack. End point security risks introduced by less mature participants in payment infrastructures can have market-wide ramifications.[37]

143. Ensuring cyber resilience as well as end point security to prevent fraud and intrusion is key to protecting the smooth functioning of the payments system. Any effective approach to tackling cyber risk should bring together the financial sector, authorities, law enforcement agencies, intelligence agencies

[36] In Hong Kong SAR, fintech firms have to apply for a virtual bank licence in order to gain access to the RTGS system and open a central bank account.

[37] As far as wholesale payment systems are concerned, the CPMI has developed a strategy to encourage and help focus industry efforts to reduce the risk of wholesale payment fraud related to end point security. The strategy is composed of seven elements designed to work holistically to address all areas relevant to preventing, detecting, responding to and communicating about fraud (CPMI (2018c)).

and other relevant authorities. Although these stakeholders will have very different roles and responsibilities, ensuring a strong coordination between them, in an integrated manner, is critical to overcoming cyber attackers. Where third parties provide critical services to payment infrastructures, those could be subjected to (indirect) oversight and/or supervision.

144. Concerted efforts are important to raise cyber maturity levels across the world given the high level of interconnectedness of the global financial system. The work of the G7 Cyber Expert Group and of international SSBs provide the necessary basis for (i) financial institutions to embed strong cyber resilience measures and (ii) authorities around the world to assess the cyber resilience of their financial institutions. Regulatory harmonisation and improvement of baseline capabilities beyond the G7 countries are important.

Box Q

## The ECB's cyber resilience expectations and red team testing

Cyber threat is borderless and the capabilities of the adversaries are constantly evolving, readily scalable and increasingly sophisticated, threatening to disrupt the interconnected global financial system. Threat actors are highly motivated and can be persistent and agile and use a variety of tactics, techniques and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. New financial technology companies are more agile and innovative, and such innovation is important for economic growth. But it is the case that such innovation, while welcome, may also bring risk as it contends with the complexity of cyber space and the threats therein.

Where these companies intersect and depend on FMIs, it is integral that FMIs operate at the highest level of cyber resilience. In this regard, a significant amount of work has already been undertaken internationally with regard to cyber risk and FMIs. In June 2016, the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures ("Guidance") was published, providing FMIs with guidance on how to establish and operationalise a cyber resilience framework. In December 2018, the ECB published the Cyber Resilience Oversight Expectations (CROE). The CROE serves the following three key purposes: (i) it provides FMIs with detailed steps on how to operationalise the Guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time; (ii) it provides overseers with clear expectations when assessing the FMIs for which they are responsible; and (iii) it provides the basis for a meaningful discussion between the FMIs and their respective overseers. The CROE sets expectations across eight categories – governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving – to ensure that FMIs are able to prevent, detect, respond to and recover from cyber attacks.

To complement the CROE, FMIs should also conduct threat intelligence-based ethical red team testing: simulated cyber attacks that mimic the TTPs of real attackers, based on bespoke threat intelligence. These simulated cyber attacks target the processes, technologies and staff of an FMI, without prior warning, in order to test its protection, detection and response capabilities. In 2018, the ECB launched the European framework for threat intelligence-based ethical red-teaming (TIBER-EU). It is the first cross-border, multi-jurisdictional, multi-regulator initiative, and has raised the standard of cyber security testing across Europe. It can be used on any type of institution and sector, and is unique in that its tests are performed on global banks and financial market infrastructures, involving many regulators on a cross-border basis.

For the exercise to run, the TIBER-EU test has to be adopted by the country's central bank as either a supervisory, a financial stability or a catalyst tool. Once adopted, financial institutions deemed core national infrastructure will be approached to conduct the test. The institution works with the TIBER team from the national authority to determine the scope of the test, after which it procures a threat intelligence and red team provider. At the end of the test, a stakeholder meeting is held to discuss the test's findings and any remediation plans. To help financial firms conduct the exercise, the ECB has also published TIBER-EU – Services Procurement Guidelines (ECB (2018a)) and TIBER-EU White Team Guidance (ECB (2018c)).

Source: ECB.

145. New technologies have the potential to enhance operational resilience and, specifically, cyber resilience. For instance, the concept of multiple synchronised ledgers and multiple processing nodes of DLT can help reduce the risk from a single point of failure. Large cloud computing providers typically have very strong measures in place to ensure operational resilience. Spreading operations geographically and multiplying the number of synchronised copies of the ledger (in the case of DLT) and backup sites (in the case of cloud computing) appears to be an effective way to deal with operational disruptions, since inoperable or compromised ledgers or nodes can be substituted. New entrants are often among the early adopters of innovative technologies, with a positive effect on security and resilience, provided those technologies are adequately tested and properly understood by market participants and authorities.

### 4.3.3 Interoperability and geographical coverage of financial infrastructures can benefit from fintech developments

146. To maximise the benefits of new technologies for financial inclusion, their adoption should not be pursued to the detriment of market integration. While fragmentation might create opportunities for specialised entities, such as payment gateways, this might be at the detriment of the overall efficiency of the retail payments market. For example, in parts of the retail payments market, the different types of new payment products created as a result of innovation have increased the complexity for payees, especially if they each have different interface requirements (CPMI (2014)). Without standardisation and harmonisation, there will be siloes and fragmentation, duplicated efforts leading to unnecessary costs, and a lack of efficiency leading to little or no gains for the unserved or underserved. Open technical standards and harmonised rules must be defined to help new technologies fulfil their promise and support market integration. Open standards and the harmonisation of legal, technical and operational aspects support the interoperability of financial infrastructures as a key feature for supporting financial inclusion (see PAFI report, Section 3.1.3.2).

147. A modular approach, allowing for infrastructure components to be flexibly stacked upon each other to build a digital infrastructure to which end users and service providers connect via APIs can foster interoperability (BIS (2020c)). While this approach is often referred to as "technology stack", the components go beyond technologies as defined in this report, but comprise infrastructures, for which reason the term "infrastructure stack" is used. The most prominent example of a technology stack is the so-called "India Stack", which provides end users with a number of services built on top of an identification layer (based on a universal biometric digital identity). It does so by bringing together five elements: (i) e-KYC; (ii) the Aadhaar Payments Bridge System (which essentially turns an Aadhaar number into the person's account identifier); (iii) eSign (a digital signature); (iv) Unified Payments Interface (a unified API enabling access to payment infrastructures for the processing of instant payments); and (v) a consent layer to share personal data (health records, financial transactions) with a bank, insurer, employer or university for a limited time for a specific purpose (IndiaStack (2020)).

148. The challenge of interoperability and geographical coverage of financial infrastructures is no longer just domestic, but is increasingly acquiring a cross-border dimension. First, the growth of domestic instant payment solutions has made the contrast with slow and expensive cross-border (retail) payments (often based on corresponding banking arrangements) even more apparent and starker (see also Section 3.4.1). Second, the expansion of proprietary systems across borders has provided a rapidly scalable solution to enable more efficient cross-border transfers (eg via electronic wallets), whereas the interlinking of domestic payment infrastructures has traditionally encountered difficulties and/or limited success. While global closed-loop solutions appear to overcome the issues arising from financial infrastructures lacking cross-border coverage and interoperability, they may lead to a situation where multiple such solutions (re)create market fragmentation issues or to a scenario where a few players dominate the market.

149. Fintech developments can support increased coverage and interoperability of financial infrastructures with a view to enhancing the efficiency and inclusiveness of cross-border payment services. Interconnecting instant payment infrastructures leveraging the SWIFT gpi initiative offers an alternative

solution that reuses existing cross-border and domestic payments networks, avoiding the complexities of new cross-border infrastructure (SWIFT (2019)). In parallel, mobile money systems are seeking to expand interoperability with each other on a regional basis (Box R). The FSB, in coordination with the CPMI and other relevant SSBs, will develop and deliver to the G20 a roadmap for how to enhance global cross-border payments in 2020 (FSB (2019c)), also taking into consideration relevant fintech developments.

150. Interoperability does not only concern payment infrastructures. Despite advances in identity and verification systems, interoperable databases are not yet the norm in many countries. Where "silo" databases cater for identification needs for specific industries (eg KYC/CDD in financial services), a "duplication of identity" is both costly and inefficient and may undermine the effectiveness of innovative verification techniques that source data from multiple databases (AFI (2019)). In several jurisdictions, financial institutions have established, or are in the process of establishing, shared facilities for customer identification in the context of domestic payments. Prompted by a large fall in correspondent banking activities in the region, the South Pacific central banks have launched an initiative to create a common KYC framework aimed at harmonising governance, technical and legal requirements for a shared KYC utility, with a view to reducing the AML/CFT compliance costs of cross-border payments (King (2020)).

Box R

## Mobile money interoperability in Sub-Saharan Africa

Several countries in Sub-Saharan Africa are undertaking efforts to increase mobile money interoperability, both within and across borders, with a view to increasing efficiency and ensuring sustainability as well as fostering financial inclusion

Nigeria Central Switch (NCS) enables mobile money operators to interoperate with banks and other financial institutions, thereby allowing them to offer a wide array of services to their customers. In 2019, mobile inter-scheme transactions grew by 470% in terms of volume and 184% in terms of value.

Ghana's Mobile Money Interoperability (MMI) platform recorded a 317% growth in the volume of transactions and 267% growth in transaction value between 2018 and 2019. MMI is the service which allows direct and seamless transfer of funds from one mobile money wallet to another across networks.

The Central Bank of West African States (BCEAO), in collaboration with the African Development Bank (ADB) and the Bill & Melinda Gates Foundation, has embarked on a project to achieve interoperability of mobile money solutions across the eight West African countries belonging to the West African Economic and Monetary Union (WAEMU). The aim is to create a common payments ecosystem for mobile network operators and, ultimately, microfinance institutions and fintech players.

With the support of the GSMA, MTN and Orange launched Mowali ("mobile wallet interoperability"). Built on top of the Bill & Melinda Gates Foundation's open-source platform Mojaloop, Mowali offers an industry-owned and industry-governed payments hub for mobile money. The service is open to any mobile money provider in Africa, as well as banks, money transfer operators and other financial service providers. Mowali is also the common mobile money acceptance brand

Sources: GHIPSS (2020); GSMA (2019b); NIBSS (2020).

# 5. Review of the PAFI guidance with focus on fintech

151. The PAFI report outlines guiding principles for achieving the payment aspects of financial inclusion objectives, and contains possible key actions for countries that want to put those guiding principles into practice. Those possible actions were based on the analysis in the PAFI report and on the experiences of countries in promoting financial inclusion. The report also noted that, as there are many differences among countries – economic, cultural and political – key actions that are helpful in one country may not be equally helpful in another. Accordingly, the suggested key actions for consideration should not be taken as a checklist of what needs to be done to foster the guiding principles.

152. The guiding principles neither prescribe nor hinge on the use of certain technologies, and hence they are not targeted at or directly informed by fintech developments. Nevertheless, the guiding principles for achieving the PAFI objectives could benefit from focused key actions for consideration by all relevant public and private sector stakeholders that seek to harness the potential of fintech while mitigating its accompanying risks. These focused actions are presented below as extensions to the original recommended key actions for consideration. For ease of reference, all key actions for consideration, including those for which additional fintech focus is not provided, are listed as well.

## Guiding principle 1: Public and private sector commitment

***Commitment from public and private sector organisations to broaden financial inclusion is explicit, strong and sustained over time.***

Most key actions for this guiding principle emphasise the importance of allocating appropriate resources to fostering financial inclusion and the need for public and private sector stakeholders to cooperate. These key actions are all the more relevant in the fintech era in light of fintech's novelty and the cross-border and/or cross-sectoral dimensions that are often involved.

*Key actions for consideration:*

- *All relevant public and private sector stakeholders support the objective that all eligible individuals – regardless of culture, gender or religion – and businesses should be able to have and use at least one transaction account, and develop an explicit strategy with measurable milestones to that end.*
    - *Fintech focus: All relevant fintech stakeholders are enlisted in support of this objective.*
- *All relevant public and private sector stakeholders allocate the appropriate human and financial resources to support financial inclusion efforts.*
    - *Fintech focus: Financial inclusion efforts seek to leverage fintech expertise among all relevant public and private sector stakeholders.*
- *Central banks, financial supervisors, regulators and policymakers effectively coordinate their efforts with regard to financial inclusion.*
    - *Fintech focus: These coordination efforts take the cross-sectoral and cross-border nature of fintech developments into consideration.*
- *Private sector stakeholders engage with relevant public sector counterparts on initiatives that promote the adoption and usage of transaction accounts, and financial inclusion more broadly.*
- *Private sector stakeholders cooperate constructively and meaningfully with each other to discuss and find solutions to issues that are best addressed by the industry as a whole.*
- *Central banks, in line with their roles, responsibilities and interests in fostering the safety and efficiency of the payments system, leverage their catalyst, oversight, supervisory and other powers as relevant and appropriate to promote financial inclusion.*

## Guiding principle 2: Legal and regulatory framework

***The legal and regulatory framework underpins financial inclusion by effectively addressing all relevant risks and by protecting consumers, while at the same time fostering innovation and competition.***

The key actions already cover a wide range of relevant risks and concerns, but fintech may exacerbate data protection and privacy concerns.. Furthermore, new approaches to regulation and the use of new technologies for risk management, compliance and financial supervision are a recent development that could be leveraged.

*Key actions for consideration:*

- *A robust framework is established to foster sound risk management practices in the payments industry, including through the supervision/oversight of PSPs and PSOs by regulatory authorities.*
    - *Fintech focus: Where appropriate, relevant authorities leverage new technologies for supervision/oversight and foster their adoption by the private sector for risk management and compliance.*
- *The framework requires PSPs and PSOs to develop and implement risk management measures that correspond to the nature of their activities and their risk profile.*
- *The framework aims to promote the use of transaction accounts in which customer funds are adequately protected through appropriate design and risk management measures, such as deposit insurance or functionally equivalent mechanisms as well as through preventive measures (eg supervision, placement of customer funds held by non-deposit-taking PSPs in high-quality and liquid assets, and, depending on the legal regime, specially protected accounts at banks and possibly trust accounts).*
    - *Fintech focus: Any new or innovative forms of transaction accounts or payment products protect customer funds through appropriate design and risk management measures that are functionally equivalent to those that protect customer funds in "traditional" deposit transaction accounts.*
- *The framework requires PSPs to clearly disclose, using comparable methodologies, all of the various fees they charge as part of their service, along with the applicable terms and conditions, including liability and use of customer data.*
    - *Fintech focus: The framework requires PSPs to clearly disclose the credit and liquidity risks that users face when storing funds in new or innovative forms of transaction accounts.*
    - *Fintech focus: The framework requires PSPs to clearly disclose how customer data are safeguarded and how data privacy is protected, along with customer rights regarding the use of their data.*
- *The framework requires PSPs to implement a transparent, user-friendly and effective recourse and dispute resolution mechanism to address consumer claims and complaints.*
- *The framework preserves the integrity of the financial system, while not unnecessarily inhibiting access of eligible individuals and businesses to well-regulated financial services.*
- *The framework promotes competition in the marketplace by providing clarity on the criteria that must be met to offer specific types of service, and by setting functional requirements that are applied consistently to all PSPs.*
- *The framework promotes innovation and competition by not hindering the entry of new types of PSP, new instruments and products, new business models or channels – as long as these are sufficiently safe and robust.*

- *Fintech focus: The framework aims to be technology-neutral by setting functional and safety requirements that are applied consistently to all PSPs.*

## Guiding principle 3: Financial and ICT infrastructures

***Robust, safe, efficient and widely reachable financial and ICT infrastructures are effective for the provision of transaction accounts services, and also support the provision of broader financial services.***

Technological innovation requires that payment infrastructures continuously review their design to ensure that they adequately support the provision of innovative payment products and access modes. Furthermore, digital ID infrastructures can play a relevant role in supporting service providers to reliably validate customers' identity.

*Key actions for consideration:*

- *Key payments infrastructures are built, upgraded or leveraged as needed to facilitate the effective usage of transaction accounts.*
    - *Fintech focus: The design of key payment infrastructures takes into account innovative technologies, products and access modes.*
- *Additional infrastructures are appropriately designed and operate effectively to support financial inclusion efforts by providing critical information to financial service providers, including an effective and efficient identification infrastructure, a credit reporting system and other data sharing platforms.*
    - *Fintech focus: Public and private sector stakeholders support the establishment of a digital ID infrastructure for customers to digitally identify, authenticate and provide consent.*
- *The geographical coverage of ICT infrastructures and the overall quality of the service provided by those infrastructures are enhanced as necessary by their owners/operators to not constitute a barrier for the provision of transaction account services in remote locations.*
- *Increased interoperability of and access to infrastructures supporting the switching, processing, clearing and settlement of payment instruments of the same kind are promoted, where this could lead to material reductions in cost and to broader availability consistent with the local regulatory regime, in order to leverage the positive network externalities of transaction accounts.*
- *Payment infrastructures, including those operated by central banks, have objective, risk-based participation requirements that permit fair and open access to their services.*
- *Financial and ICT infrastructures leverage the broad usage of open/non-proprietary technical standards, harmonised procedures and business rules to enhance their efficiency and therefore their ability to support transaction accounts at low costs.*
- *The safety and reliability of financial and ICT infrastructures, including their resilience against fraud, are tested on an ongoing basis and are enhanced as necessary to keep up with all emerging threats for holders of transaction accounts, PSPs and PSOs.*

## Guiding principle 4: Transaction account and payment product design

***The transaction account and payment product offerings effectively meet a broad range of transaction needs of the target population, at little or no cost.***

As transaction account and payment product design evolve as a result of technological innovation, affordability and functionality remain paramount. Innovations in product design could lead to the financial exclusion of disadvantaged segments of the population.

*Key actions for consideration:*

- *Where reasonable and appropriate, PSPs provide a basic transaction account at little or no cost to all individuals and businesses that do not hold such an account and that wish to open such an account.*
- *PSPs offer transaction accounts with functionalities that, at a minimum, make it possible to electronically send and receive payments at little or no cost, and to store value safely.*
    - *Fintech focus: PSPs leverage new technologies and access modes to improve the design of transaction accounts and payment products for the benefit of all their customer segments.*
- *PSPs leverage efficient and creative approaches and effective management practices in their efforts to offer transaction accounts and functionalities in a commercially viable and sustainable way.*
- *The payment services industry, operators of large-volume payment programmes and other stakeholders recognise that the payment habits and needs of currently unserved and underserved customers are likely to differ, and therefore engage in market research and/or other similar efforts to identify and address those payment habits and needs.*
    - *Fintech focus: The development and adoption of new technologies, products and access modes avoids the exclusion of customer segments due to factors such as age, culture, gender, religion and financial literacy.*
- *PSPs work to ensure that the payment needs of the private and public sector entities with whom holders of transaction accounts regularly conduct payments are met as well.*
- *PSPs work to ensure that the products that target unserved or underserved population segments are easy to use.*
- *PSP efforts to continuously improve their transaction account offering include both traditional and innovative payment products and instruments.*

## Guiding principle 5: Readily available access points

***The usefulness of transaction accounts is augmented with a broad network of access points that also achieves wide geographical coverage, and by offering a variety of interoperable access channels.***

With new technologies, low-cost access channels have become available, which have the potential to increase the acceptance of payment instruments and widen the available access points. At the same time, the increasing reliance on digital channels and reduced availability of cash in some countries could hamper the wide availability of access points.

*Key actions for consideration:*

- *PSPs provide convenient access to transaction accounts and services by offering an effective combination of own and third-party-owned physical access points (eg branches, ATMs, POS terminal networks and PSP agent locations) and of remote/electronic access channels (mobile phones, internet banking, etc).*
    - *Fintech focus: PSPs seek to leverage the potential of new technologies, products and access modes to offer low-cost, easy-to-use access points and channels to expand reach and acceptance of electronic payment instruments, while ensuring that a basic level of physical access points is maintained.*
- *PSPs work to provide service levels at various access points and channels that are reliable and of high quality (PSP agents have the necessary liquidity and are equipped with effective tools to service*

*transaction account users reliably and in an efficient manner, ATMs are highly reliable, etc) and to ensure that opening hours are broadly aligned with customers' transacting needs.*

- *The payments industry works on ensuring that access points and channels are appropriately interoperable, further contributing to expanding the reach of available service access points and the overall convenience to holders of transaction accounts.*
- *PSPs adequately train their own front office staff and their agents to understand and appropriately address cultural, gender and religious diversity when servicing holders of transaction accounts.*
- *The payments industry and authorities monitor access channels and access points and their usage to obtain an accurate picture of the availability and proximity of service points to the different population segments.*
    - *Fintech focus: The payments industry and authorities consider the impact of the continued decline in the use of cash and the reduction in the availability and proximity of cash access points.*

## Guiding principle 6: Awareness and financial literacy

***Individuals gain knowledge, through awareness and financial literacy efforts, of the benefits of adopting transaction accounts, how to use those accounts effectively for payment and store-of-value purposes, and how to access other financial services.***

As the lack of digital capabilities may hinder access to and use of certain innovative forms of transaction accounts and payment products, awareness and financial literacy efforts could usefully include elements of new technologies to instil the relevant competencies.

*Key actions for consideration:*

- *All relevant public and private sector stakeholders engage in ongoing and effective educational and outreach to support awareness and financial literacy with an appropriate degree of coordination.*
    - *Fintech focus: Educational and outreach efforts support awareness and financial literacy with respect to new technologies, products and access modes, using both traditional and digital communication means.*
- *Awareness and financial literacy efforts specifically address how payment and store-of-value needs can be met through the usage of transaction accounts. In this context, individuals that do not have a transaction account and those that obtained one only recently are a primary target of these financial literacy efforts.*
- *Awareness and financial literacy efforts make it possible to easily obtain clear and accurate information on the various types of account that are available in the market, on the general account opening requirements, and on the types of account and service fee that may be encountered.*
- *Awareness, financial literacy and financial transparency programmes make it possible for transaction account users to easily obtain clear and accurate information on the risks embedded in the usage of these accounts, how the costs in using the associated services can be minimised, how the potential benefits can be maximised, the basic security measures associated with these accounts, and the overall obligations and rights of PSPs and users.*
- *PSPs provide hands-on training where needed as part of a product rollout, particularly for users with limited first-hand exposure to electronic payment services and the associated technologies (eg PSPs show customers how transaction accounts and the associated payment products work in practice).*

## GP 7: Large-volume, recurrent payment streams

***Large-volume and recurrent payment streams, including remittances, are leveraged to advance financial inclusion objectives, namely by increasing the number of transaction accounts and stimulating the frequent usage of these accounts.***

Large-volume and recurrent payment streams provide opportunities to promote financial inclusion. For example, transit payments and international remittances are still largely untapped, whereas fintech developments offer the opportunity to overcome current barriers to effectively use transaction accounts for these purposes.

*Key actions for consideration:*

- *Ad hoc incentives are considered, where appropriate, to foster adoption and usage of transaction accounts for large-volume and recurrent payments, including not only government payment programmes but also government collections and utility bill payments, transit fare payments, employer payrolls and, where relevant, remittances.*
    - *Fintech focus: New technologies, products and access modes that facilitate the use of account-based, open-loop payment methods for large-volume and recurrent payments are considered.*
- *PSOs and PSPs take into consideration the needs and requirements of the key counterparties involved in large-volume payment streams, such as employers, large-volume billers, the national treasury and others in the design and provision of the related payment services.*
- *The government considers making its G2P and G2B payments through a choice of competitively offered transaction accounts that meet the payment and store-of-value needs of the recipients so that these accounts are useful to them.*
- *The government enables and encourages individuals and businesses to make their P2G and B2G payments through electronic means in order to, among other objectives, increase the overall usefulness of transaction accounts.*
- *Medium-sized and large firms, along with government entities, consider disbursing salaries and other payments to employees via transaction accounts at the PSP of the employees' choice.*
- *The payments industry proactively seeks new ways to make transaction accounts a competitive and convenient option for usage in connection with all large-volume payment streams.*
    - *Fintech focus: All relevant stakeholders take into consideration the potential of new technologies, products and access channels to improve the current offerings of cross-border retail payment services with a view to making transaction accounts more attractive for sending and receiving international payments, including remittances.*

# 6. Conclusions

153. Technological innovation and payments are intertwined. The developments currently observed in the fintech era are not new per se, but have unprecedented depth and speed to them, which has raised authorities' expectations with regard to fintech's potential to support financial inclusion objectives.

154. This report shows that fintech offers opportunities to underpin the drivers of access to and usage of transaction accounts as identified in the context of the PAFI report, namely: (i) transaction account and payment product design; (ii) access points; (iii) awareness and financial literacy; and (iv) large-volume recurrent payment streams – albeit to different degrees. Yet fintech is not without challenges, and if risks are not properly managed, they can undermine financial inclusion outcomes. The relevant stakeholders must strike the right balance between: increasing efficiency while ensuring safety; enhancing customer experience and protecting the consumer and data privacy; achieving ubiquity and avoiding digital exclusion; and lowering market entry barriers and addressing concentration risks.

155. The PAFI foundations – (i) public and private sector commitment; (ii) legal and regulatory framework; and (iii) financial and ICT infrastructures – can play a critical role in ensuring a balanced approach. Stronger emphasis should be placed, inter alia, on enhancing international and cross-sectoral coordination between authorities; clarifying the applicability of existing regulatory and oversight requirements, and addressing any gaps that may arise; and fostering the resilience and availability of payment and ICT infrastructures.

156. In conclusion, the PAFI report provides a useful framework for incorporating and leveraging fintech's opportunities for increasing access to and use of transaction accounts, while addressing the challenges. However, it will take an explicit, concerted effort to seize fintech's potential for achieving the PAFI objectives.

# Annex A: Members of the task force

**Co-Chairs of the Task Force**

| | |
|---|---|
| Bank for International Settlements | Marc Hollanders |
| World Bank Group | Harish Natarajan |

**Co-leads of the fintech workstream**

| | |
|---|---|
| European Central Bank | Maria Teresa Chimienti |
| European Central Bank (until October 2019) | Thomas Lammer |
| Bank for International Settlements (from November 2019) | |

**Members of the PAFI Task Force**

| | |
|---|---|
| Arab Monetary Fund | Habib Attia |
| Bank Indonesia | Aida Fitri |
| | Budi Widihartanto (until June 2019) |
| | Marlina Alen (from July 2019) |
| Bank of Albania | Ledia Bregu |
| Bank of Italy | Paola Giucca |
| | Angela Caporrini |
| Bank of Korea | Jaekwang Roh (until August 2019) |
| | Young Sun Yoo (from September 2019) |
| Bank of Mexico | Miguel Díaz |
| Bank of Morocco | Hakima El-Alami |
| Central Bank of the Russian Federation | Nadezhda Prasolova |
| | Pavel Sumbulov |
| Center for Latin American Monetary Studies | Raúl Morales |
| Central Bank of Brazil | Luis Gustavo Mansur Siqueira |
| Central Bank of the Republic of Argentina | Pablo García Arabehety |
| Central Bank of the Republic of Turkey | Güzide Merve Öztürk |
| Central Bank of West African States | Gisele C Keny Ndoye |
| Deutsche Bundesbank | Johannes Gerling |
| | Johannes Klocke |
| European Central Bank | Daniela Russo |
| | Patrick Papsdorf |

| | |
|---|---|
| Federal Reserve Bank of New York | Adrienne Manns |
| | Sishush Maru |
| Hong Kong Monetary Authority | Mok Man Kit |
| International Monetary Fund | Ananthakrishnan Prasad |
| People's Bank of China | He Zhenggen |
| | Chang Jing |
| Reserve Bank of India | Amitabh Khandelwal |
| Saudi Arabian Monetary Authority | Abdullah Alsoyan |
| South African Reserve Bank | Magedi-Titus Thokwane |
| State Bank of Vietnam | Le Anh Dung |
| World Bank Group | Oya Pinar Ardic Alper |

**Secretariat**

| | |
|---|---|
| World Bank Group | José Antonio García |

## Annex B: Acronyms and abbreviations

| | |
|---|---|
| AE | advanced economy |
| AFA | additional factor of authentication |
| AFI | Alliance for Financial Inclusion |
| AFIN | ASEAN Financial Innovation Network |
| AI | artificial intelligence |
| AISP | account information service provider |
| AML | anti-money laundering |
| API | application programming interface |
| ATM | automated teller machine |
| ASEAN | Association of Southeast Asian Nations |
| B2B | business-to-business |
| B2G | business-to-government |
| BaaS | banking as a service |
| BCBS | Basel Committee on Banking Supervision |
| BiM | Billetera Móvil |
| BIS | Bank for International Settlements |
| BLE | bluetooth low-energy |
| CBDC | central bank digital currency |
| CDD | customer due diligence |
| CEMLA | Centro de Estudios Monetarios Latinoamericanos (Center for Latin American Monetary Studies) |
| CFT | countering/combating the financing of terrorism |
| CGAP | Consultative Group to Assist the Poor |
| CICO | cash-in/cash-out |
| CKYCR | Central KYC Records Registry |
| CPF | countering proliferation financing |
| CPMI | Committee on Payments and Market Infrastructures |
| DL | deep learning |
| DLT | distributed ledger technology |
| EBA | European Banking Authority |
| ECB | European Central Bank |
| e-commerce | electronic commerce |
| EEA | European Economic Area |
| EFT | electronic funds transfer |
| e-ID | electronic identification |
| e-KYC | electronic know-your-customer |
| EMDE | emerging market and developing economy |
| EMI | electronic money issuer |
| e-money | electronic money |
| EPC | European Payments Council |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| FATF | Financial Action Task Force |

| | |
|---|---|
| FCA | Financial Conduct Authority |
| FIDO Alliance | Fast Identity Online Alliance |
| FIG | Financial Innovation Group |
| FINMA | Financial Market Supervisory Authority |
| FMI | financial market infrastructure |
| FSB | Financial Stability Board |
| FSI | Financial Stability Institute |
| FTI | financial technology institution |
| G7 | Group of Seven |
| G20 | Group of Twenty |
| G2B | government-to-business |
| G2P | government-to-person |
| GhIPSS | Ghana Interbank Payment Settlement Systems |
| GSM | global system for mobile communications |
| GSMA | GSM Association |
| ICT | information and communication technology |
| ID4D | Identification for Development |
| IMF | International Monetary Fund |
| IOSCO | International Organization of Securities Commissions |
| IoT | internet of things |
| ISO | International Organization for Standardization |
| KYC | know-your-customer |
| LEI | Legal Entity Identifier |
| MAS | Monetary Authority of Singapore |
| ML | machine learning |
| MNO | mobile network operator |
| MSME | micro-, small and medium-sized enterprise |
| MST | magnetic secure transmission |
| NBFI | non-bank financial institution |
| NFC | near field communication |
| NIBSS | Nigeria Inter-Bank Settlement System |
| NIST | National Institute of Standards and Technology |
| NPCI | National Payments Corporation of India |
| NPP | new payments platform |
| OECD | Organisation for Economic Co-operation and Development |
| PaaS | payment as a service |
| PAFI | payment aspects of financial inclusion |
| PAN | primary account number |
| PAYG | pay-as-you-go |
| PFMI | Principles for Financial Market Infrastructure |
| PIN | personal identification number |
| PISP | payment initiation service provider |
| POS | point of sale |
| PSD2 | Revised Payment Services Directive |
| PSO | payment system operator |

| | |
|---|---|
| PSP | payment service provider |
| QR | quick response |
| RBA | Reserve Bank of Australia |
| RBI | Reserve Bank of India |
| RFID | radio frequency identification |
| RSP | remittance service provider |
| RTGS | real-time gross settlement |
| SCA | strong customer authentication |
| SEPA | Single Euro Payments Area |
| SCT | SEPA Credit Transfer |
| SCT Inst | Instant SEPA Credit Transfer |
| SDG | Sustainable Development Goal |
| SIC | Swiss Interbank Clearing |
| SIM | subscriber identification module |
| SME | small and medium-sized enterprise |
| SNB | Swiss National Bank |
| SSB | standard-setting body |
| SSID | self-sovereign identity |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| TF | terrorist financing |
| TfL | Transport for London |
| TPP | third-party provider |
| TSP | token service provider |
| UIDAI | Unique Identification Authority of India |
| UNSGSA | United Nations Secretary-General's Special Advocate for Inclusive Finance for Development |
| UPI | Unified Payments Interface (India) |
| USSD | Unstructured Supplementary Service Data |
| WBG | World Bank Group |
| WEF | World Economic Forum |

# Annex C: References


Access to Cash Review (2019): *Access to Cash Review Final Report*, March, https://www.accesstocash.org.uk/media/1087/final-report-final-web.pdf.

Adrian, T and T Mancini Griffoli (2019): "The rise of digital money", *FinTech Notes*, no 19/001, International Monetary Fund, 15 July, https://www.imf.org/~/media/Files/Publications/FTN063/2019/English/FTNEA2019001.ashx.

Alliance for Financial Inclusion (AFI) (2019): "KYC innovations, financial inclusion and integrity in selected AFI member countries", *AFI Special Report*, March.

APIX (2020): "APIX platform – about us", https://apixplatform.com/aboutapix.

Appaya, S and I Jenik (2019): *Regulatory Sandbox Global Survey: summary results*, CGAP and World Bank.

Australian Treasury (2019): *Consumer data right: overview*, September.

Aveni, T J and J Roest (2017): *China's Alipay and WeChat Pay: reaching rural users*, CGAP, 1 December, http://documents.worldbank.org/curated/en/451921533193590101/China-s-Alipay-and-WeChat-Pay-reaching-rural-users.

Bahia, K and S Suardi (2019): *The state of mobile internet connectivity*, GSM Association, July.

Bank for International Settlements (2020a): BIS Innovation Hub, https://www.bis.org/topic/fintech/hub.htm.

——— (2020b): "Central bank group to assess potential cases for central bank digital currencies", press release, 21 January, https://www.bis.org/press/p200121.htm.

——— (2020c): *How are authorities responding to fintech? A cross-country analysis*, forthcoming.

Bank of England (2016): "Enabling the FinTech transformation – revolution, restoration, or reformation?", speech by Mark Carney, 16 June. https://www.bis.org/review/r160621e.pdf

——— (2018): "First non-bank payment service provider (PSP) directly accesses UK payment system", media release, 18 April.

——— (2018): *Sound Practices: implications of fintech developments for banks and bank supervisors*, February.

——— (2019): *Report on open banking and application programming interfaces*, November, https://www.bis.org/bcbs/publ/d486.pdf.

——— (2020): "It's time to talk about money. Speech at the London School of Economics", speech by Jon Cunliffe, 28 February. https://www.bankofengland.co.uk/-/media/boe/files/speech/2020/its-time-to-talk-about-money-speech-by-jon-cunliffe.pdf?la=en&hash=A39E014DBBA2C5E88D1B8339E61598CBD62BCA3E

Bazarbash, M (2019): "FinTech in financial inclusion: machine learning applications in assessing credit risk", *IMF Working Papers*, no WP/19/109, May, https://www.imf.org/~/media/Files/Publications/WP/2019/WPIEA2019109.ashx.

BBVA (2018): *Digital Economy Outlook*, March.

——— (2019): "Mobile onboarding outstrips other digital channels for new signups at BBVA", *Finextra*, https://www.finextra.com/pressarticle/77669/mobile-onboarding-outstrips-other-digital-channels-for-new-signups-at-bbva.

Bech, M and J Hancock (2020): "Innovations in payments", *BIS Quarterly Review*, March.

Berkmen, P, K Beaton, D Gershenson, J Arze del Granado, K Ishi, M Kim, E Kopp and M Rousset (2019): "Fintech in Latin America and the Caribbean: stocktaking", *IMF Working Papers*, no WP/19/71, March, https://www.imf.org/~/media/Files/Publications/WP/2019/WPIEA2019071.ashx.

Bijlsma, M, C van der Cruijsen and N Jonker (2020): *Consumer propensity to adopt PSD2 services: trust for sale?*, Netherlands Bank and Tilburg University, January, https://www.dnb.nl/en/binaries/Working%20paper%20No.%20671_tcm47-387219.pdf.

Boar, C, H Holden and A Wadsworth (2020): "Impending arrival – a sequel to the survey on central bank digital currency", *BIS Working Papers*, no 107, January, https://www.bis.org/publ/bppdf/bispap107.pdf.

Boston Consulting Group (BCG) (2019): "Tapping into the pockets of growth", *Global Payments 2019*, http://image-src.bcg.com/Images/BCG-Global-Payments-2019-Tapping-into-Pockets-of-Growth-September-2019-rev_tcm20-231986.pdf.

Broeders, D and J Prenio (2018): "Innovative technology in financial supervision (suptech) – the experience of early users", *FSI Insights on policy implementation*, no 9, Financial Stability Institute, July.

Bullmann, D, J Klemm and A Pinna (2019): "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper Series*, no 230, August.

Cambridge Centre for Alternative Finance (CCAF) and World Economic Forum (WEF) (2020): *Transforming paradigms: a global AI in financial services survey*, January, http://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf.

Centre for Financial Inclusion (Cenfri) (2019): *Regulating for innovation: an evolving framework*, August.

Centro de Estudios Monetarios Latinoamericanos (CEMLA) (2019): *Key Aspects around Financial Technologies and Regulation Policy report*, May, https://www.cemla.org/fintech/docs/2019-06-KeyAspectsAroundFinancialTechandRegulation.pdf.

——— (2020): Forum of FINTECH Experts, https://www.cemla.org/fintech/english.html.

Chen, G, A Fiorillo and M Hanouch (2016): "Smartphones & mobile money: principles for UI/UX design (1.0)", CGAP, October.

Chiampo, M, J Roest and A Raman (2018): "QR codes and financial inclusion: reasons for optimism", CGAP, January.

Chimienti, M, U Kochanska and A Pinna (2019): "Understanding the crypto-asset phenomenon, its risks and measurement issues", *ECB Economic Bulletin*, issue 5/2019, August.

Cleland, V and G Hartsink (2020): "The value of the Legal Entity Identifier for the payments industry", *Journal of Payments Strategy & Systems*, vol 13, no 4, Winter 2019–20, pp 322–36.

Coelho, R, M De Simoni and J Prenio (2019): "Suptech applications for anti-money laundering", *FSI Insights on policy implementation*, no 18, Financial Stability Institute, August.

Committee on Payments and Market Infrastructures (2014): *Non-banks in retail payments*, September.

——— (2015): *Digital currencies*, November.

——— (2016): *Fast payments*, November.

——— (2017a): *Distributed ledger technology in payment, clearing and settlement – an analytical framework*, February.

——— (2018a): *Cross-border retail payments*, February.

——— (2018b): *Central bank digital currencies*, March.

——— (2018c): *Reducing the risk of wholesale payments fraud related to endpoint security*, May, https://www.bis.org/cpmi/publ/d178.pdf.

——— (2019a): Analysis of the 2018 Red Book Statistics, November.

——— (2019b): Red Book statistics for CPMI countries, November.

Committee on Payment and Market Infrastructures and World Bank (2016): *Payment aspects of financial inclusion*, April.

Consultative Group to Assist the Poor (CGAP) (2019): "China: a digital payments revolution", Research & Analysis Publication, September.

Cuen, L (2020): "Bitcoin usage among merchants is up, according to data from Coinbase and BitPay," *Coindesk*, 3 February, https://www.coindesk.com/bitcoin-usage-among-merchants-is-up-according-to-data-from-coinbase-and-bitpay.

Cuervo, C, A Morozova and N Sugimoto (2020): "Regulation of crypto assets", *FinTech Notes*, no 19/03, International Monetary Fund, 10 January, https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Regulation-of-Crypto-Assets-48810.

Danmarks Nationalbank (2017): "Danish households opt out of cash payments", *Analysis*, no 24, December.

——— (2019): "Danes have become contactless payers", *Statistics*, 2 December.

Davidović, S, E Loukoianova, C Sullivan and H Tourpe (2019): "Strategy for fintech applications in the Pacific Island countries", International Monetary Fund, *Departmental Papers / Policy Papers*, August, https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/08/21/Strategy-for-Fintech-Applications-in-the-Pacific-Island-Countries-46862.

De Nederlandsche Bank (DNB) (2019): *General principles for the use of artificial intelligence in the financial sector*.

De Nederlandsche Bank (DNB) and Dutch Payments Association (DPA) (2018): "From cash to cards – how debit card payments overtook cash in the Netherlands", *Occasional Studies*, no 16, Amsterdam.

Deloitte (2017): "Power Up: UK business – collaborate to boost UK growth".

Demirgüç-Kunt, A, L Klapper, D Singer, S Ansar and J Hess (2018): *The Global Findex Database 2017: measuring financial inclusion and the fintech revolution*, World Bank.

Department of Finance Canada (2019): *A review into the merits of open banking*, January, https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html.

di Castri S, M Grasser and A Kulenkampff (2018): "Financial authorities in the era of data abundance – RegTech for regulators and SupTech solutions", FA, RegTech for Regulators Accelerators (R2A), Somerville MA, August.

di Castri, S, S Hohl, A Kulenkampff and J Prenio (2019), "The suptech generations", *FSI Insights on policy implementation*, no 19, Financial Stability Institute, October.

Dias, D (2020): "How Can Licensing Regimes Keep Up with Financial Innovation in 2020?", 26 February, https://www.cgap.org/blog/how-can-licensing-regimes-keep-financial-innovation-2020.

Dias, D and J C Izaguirre (2019): "Regulator's friend or foe? Cloud computing in financial inclusion", CGAP, 16 September, https://www.cgap.org/blog/regulators-friend-or-foe-cloud-computing-financial-inclusion.

D'Silva, D, Z Filková, F Packer and S Tiwari (2019): "The design of digital financial infrastructure: lessons from India", *BIS Papers*, no 106, December.

EHI Retail Institute (2019): "Love for cash is waning", 5 July.

Ehrentraud, J, D García Ocampo, L Garzoni and M Piccolo (2020): "Policy responses to fintech: a cross-country overview", *FSI Insights on policy implementation*, no 23, Financial Stability Institute, January, https://www.bis.org/fsi/publ/insights23.pdf.

Euro Banking Association (2019): *Best practices to support PSPs in detecting/combatting fraud and scam*.

European Banking Authority (EBA) (2017): *Recommendations on outsourcing to cloud service providers*, EBA/REC/2017/03, December.

——— (2018): *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, June, https://eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf?retry=1.

——— (2020): *EBA Report on big data and advanced analytics*, EBA/REP/2020/01, January.

European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA) (2018): *Joint Committee Final Report on Big Data*, March.

European Central Bank (ECB) (2017): "The use of cash by households in the euro area", *Occasional Paper Series*, no 201, November.

——— (2018a): *TIBER-EU Framework Services Procurement Guidelines*, August. https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf

——— (2018b): *Fifth report on card fraud*, 26 September.

——— (2018c): *TIBER-EU White Team Guidance*, December. https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf

——— (2019a): "Crypto-assets: implications for financial stability, monetary policy, and payments and market infrastructures", *Occasional Paper Series*, no 223, May.

——— (2019b): "Exploring anonymity in central bank digital currencies", *In Focus*, no 4, December, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf.

European Central Bank (ECB) and Bank of Japan (BoJ) (2019): *Synchronised cross-border payments*, June.

European Payments Council (EPC) (2019): Non-NFC based mobile SEPA Card proximity payments, June.

European Parliament (2018): *Competition issues in the area of financial technology (FinTech)*, July.

European Telecommunications Standards Institute (ETSI) (2011): Radio Frequency Identification (RFID), https://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf

Feyen, E, J Frost and H Natarajan (2020): "Digital money: implications for emerging market and developing economies", *Vox*, 16 January.

FIBR (2018): *Artificial intelligence: practical superpowers – the case for AI in financial services in Africa*, May.

Financial Action Task Force (FATF) (2014): "FATF clarifies risk-based approach: case-by-case, not wholesale de-risking", media release, 24 October.

——— (2020): *Guidance on digital identity*, 6 March, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf.

Financial Conduct Authority (2018): "FCA introduces new rules on handling complaints about Authorized Push Payment fraud", media release, 14 December.

Financial Stability Board (2017): *Financial stability implications from FinTech – supervisory and regulatory issues that merit authorities' attention*, June.

——— (2019a): *FinTech and market structure in financial services – market developments and potential financial stability implications*, February.

——— (2019b): "FSB sets out work to consider regulatory issues of stablecoins", media release, 18 October.

——— (2019c): *FSB work programme for 2020*, 17 December.

——— (2019d): *BigTech in finance – market developments and potential financial stability implications*, December.

Finextra (2020a): "Digital payments overtake cash in Russia", newsletter, 3 February, https://www.finextra.com/newsarticle/35209/digital-payments-overtake-cash-in-russia?utm_medium=dailynewsletter&utm_source=2020-2-4&member=107678.

——— (2020c): "UK consumers bearing the cost of cash machine fee hikes", newsletter, 7 February. https://www.finextra.com/newsarticle/35249/uk-consumers-bearing-the-cost-of-cash-machine-fee-hikes?utm_medium=dailynewsletter&utm_source=2020-2-10&member=107678

Ghana Interbank Payment Settlement Systems (GHIPSS) (2020): gh-link. https://ghipss.net/products-services/gh-link.

Global Partnership for Financial Inclusion (GPFI) (2016): *G20 High-Level Principles for Digital Financial Inclusion*, https://www.gpfi.org/sites/gpfi/files/documents/G20%20High%20Level%20Principles%20for%20Digital%20Financial%20Inclusion%20-%20Full%20version-.pdf.

Global Partnership for Financial Inclusion and Organisation for Economic Co-operation and Development (2019): *G20 Fukuoka Policy Priorities on Aging and Financial Inclusion*.

Grady, R, F Montes and M Traversa (2018): *Financial consumer protection and new forms of data processing beyond credit reporting*, World Bank Group and Ministry of Foreign Affairs of the Netherlands, November.

Greenham, T and F Travers-Smith (2019): "Cashing Out: The hidden costs and consequences of moving to a cashless society", January. https://www.thersa.org/CashingOut

Group of Seven, International Monetary Fund and Committee on Payments and Market Infrastructures (2019): *Investigating the impact of global stablecoins*, October.

GSM Association (2018a): *Competing with informal channels to accelerate the digitization of remittances*, May.

——— (2018b): *Distribution 2.0 – the future of mobile money agent distribution networks*, July.

——— (2018c): *Guidance on mobile money data protection*, September.

——— (2019a): *Access to Mobile Services and Proof of Identity 2019 – assessing the impact on digital and financial inclusion*, 22 February.

——— (2019b): *2018 State of the Industry Report on Mobile Money*, 25 February.

Gurung, N and L Perlman (2018): *Use of regtech by central banks and its impact on financial inclusion*.

He, D, R Leckow, V Haksar, T Mancini-Griffoli, N Jenkinson, M Kashima, T Khiaonarong, C Rochon and H Tourpe (2017): *Fintech and financial services – initial considerations*, International Monetary Fund, June.

Hernandez, E (2019): *Agent networks at the last mile – a guide for digital finance to reach rural customers*, CGAP, November, https://www.cgap.org/sites/default/files/publications/2019_11_Technical_Guide_Agent_Networks_Last_Mile_0.pdf.

IndiaStack (2020): "What is the India Stack?", https://www.indiastack.org/about/.

Institute of International Finance (IIF) (2018): *Liability and consumer protection in open banking*, September.

International Monetary Fund and World Bank (2018): "The Bali Fintech Agenda", *Policy Papers*, October.

——— (2019): "Fintech – the experience so far", *Policy Papers*, no 19, June.

ITU-T Focus Group Digital Financial Services (2016): *Access to payment infrastructures*, August.

Izaguirre, J C, D Dias and M Kerse (2019): *Deposit insurance treatment of e-money – an analysis of policy choices*, CGAP, October.

Jenik, I and K Lauer (2017): *Regulatory sandboxes and financial inclusion*, CGAP, October.

Jenik, I and P Zetterli (2020): *Digital Banks: How can they deepen financial inclusion?*, CGAP, February. https://www.cgap.org/research/slide-deck/digital-banks-how-can-they-deepen-financial-inclusion

Khiaonarong, T and T Goh (2020): "Fintech and payments regulation – analytical framework", *IMF Working Papers*, forthcoming.

King, M (2019): "The competitive threat from TechFins and BigTech in financial services", in Michael King and Richard Nesbitt (eds), *The technological revolution in financial services*, University of Toronto Press, forthcoming.

King, R (2020): "KYC initiative could help stem correspondent banking decline", *Central Banking*, January.

Kipkemboi, K, J Woodsome and M Pisa (2019): *Overcoming the Know Your Customer hurdle – innovative solutions for the mobile money sector*, GSM Association.

Leong, C, D Bachenheimer, D Preston and J Alexander (2018): *Imprint your future – biometric authentication in the new digital world*, Accenture Consulting, https://www.accenture.com/_acnmedia/PDF-79/Accenture-Biometric-authentication-new-digital-world-for-banking.pdf#zoom=50.

Lewis, L (2019): "Japan's quest for cashless payments", *Financial Times*, 23 December.

Lukonga, I (2018): "Fintech, inclusive growth and cyber risks – a focus on the MENAP and CCA regions", *IMF Working Papers*, no WP/ 18/201, September, https://www.imf.org/~/media/Files/Publications/WP/2018/wp18201.ashx.

Manikandan, A (2019): "Tech norms for Account Aggregator ecosystem out", *Economictimes*, 14 November.

McKinsey & Company (2019): *Global Payments Report 2019 – amid sustained growth, accelerating challenges demand bold actions*, September, https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/tracking%20the%20sources%20of%20robust%20payments%20growth%20mckinsey%20global%20payments%20map/global-payments-report-2019-amid-sustained-growth-vf.ashx.

Mejía-Ricart, R, C Tellez and M Nicoli (2019): "Paying across borders – can distributed ledgers bring us closer together?", *World Bank Blogs*, 26 March.

Mell, P and T Grance (2011): "The NIST definition of cloud computing", *Special Publication* 800-145, National Institute of Standards and Technology, September.

Mihet, R (2019): *Who benefits from innovations in financial technology?*, December, https://ssrn.com/abstract=3474720.

Mittal, A (2018): Catalog of Technical Standards for Digital Identification Systems, World Bank Group.

Monetary Authority of Singapore (MAS) (2018): H1 2018 Retail Payment Statistics for Selected Payment Systems in Singapore.

Morgan, J (2014): "A simple explanation of the 'Internet of Things'", *Forbes*, May.

Murthy, G and D Medine (2018): "Data protection and financial inclusion – why consent is not enough", CGAP, December, https://www.cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough.

Murthy, G, M Fernández-Vidal, X Faz and R Barreto (2019): *Fintechs and financial inclusion*, CGAP, May.

Natarajan, H, M Appaya and S Balasubramanian (2018): *G20 digital identity onboarding*, World Bank Group.

Natarajan, H, S Krause and H Gradstein (2017): "Distributed ledger technology (DLT) and blockchain", *FinTech Notes*, no 1, World Bank Group.

National Payments Corporation of India (NPCI) (2019): "UPI crosses 1 BN transactions in October 2019", press release,
1 November.

——— (2020): Bharat QR FAQs, https://www.npci.org.in/bharatqr-faq-%20s.

Near Field Communication (NFC) Forum (2013): "How is NFC different from or related to other wireless/RF technologies?", 17 December.

Nigeria Inter-Bank Settlement System (NIBSS) (2020): Mobile (interscheme) transfers, https://nibss-plc.com.ng/mobile-interscheme-transfers/.

Noonan, L (2019), "Banks use fintech to make up for lost time on financial inclusion", *Financial Times*, 24 April.

Norges Bank (2019): "Retail payment services 2018", *Norges Bank Papers*, no 1, May.

Organisation for Economic Co-operation and Development (2018): *G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy*.

——— (2018b): *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age*.

Parulava, S (2017): *Blockchains, distributed ledgers and funds transfer – an overview*, FSD Africa.

Peachey, K (2019): "Consumers' credit card spending 'overtakes cash'", BBC News, 19 September.

Petralia, K, T Philippon, T Rice and N Véron (2019): "Banking disrupted? Financial intermediation in an era of transformational technology", *Geneva Report on the World Economy*, no 22.

PwC Financial Services (2018): *Opening the bank for a new era of growth*, June.

Rai, S (2020): "India's about to hand people data Americans can only dream of", Bloomberg, 12 January.

Reserve Bank of Australia (2019): *NPP functionality and access consultation – conclusions paper*, June.

Reserve Bank of India (RBI) (2019): Payment and Settlement Systems in India: Vision – 2019-2021. *E*mpowering Exceptional (*E*)payment *E*xperience, https://m.rbi.org.in/Scripts/PublicationVisionDocuments.aspx?Id=921.

——— (2020): Websites of Indian banks, https://www.rbi.org.in/scripts/banklinks.aspx.

Robbins, J (2019): "Taking a ferry to the ATM: which areas face the longest treks to a free cash machine?", *Which?*, October.

Rolfe, A (2018): "The rise of digital and mobile wallet – global usage statistics from 2018", *Payments Cards & Mobile*, 26 November.

Rowntree, O (2018): *Connected women – the Mobile Gender Gap Report 2018*, GSM Association.

Roy, R and S Rai (2017): "Digitalization in India", in IMF, *Digital revolutions in public finance*, November.

Ruehl, M and J Kynge (2019): "Fintech: the rise of the Asian 'super app'", *Financial Times*, 12 December.

Santoro, M, L Vaccari, D Mavridis, R Smith, M Posada and D Gattwinkel (2019): *Web Application Programming Interfaces (APIs) – general-purpose standards, terms and European Commission initiatives*, European Commission, Joint Research Centre, Digital Economy Unit, Ispra, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118082/jrc118082_api-landscape-standards_v29_1.pdf.

Schiff, A and M McCaffrey (2017): *Redesigning digital finance for big data*, MicroSave Helix Institute of Digital Finance.

Shaw, G (2019): "Bank branch closures – is your local bank closing?", *Which?*, November.

Shrader, L (2014): *Killer apps in China – social networks and financial inclusion*, CGAP.

Society for Worldwide Interbank Financial Telecommunication (SWIFT) (2019): "SWIFT sees success with instant cross-border payments through Singapore's FAST", July.

Sorensen, E (2019): "QR code payments – what is it and how does it work?", *Mobile Transaction*, 4 September.

Stoorvogel, A (2019): "NFC, QR codes, In-App and beyond…", *Payments Journal*, 10 January.

Sveriges Riksbank (2018): "Considerations for a cashless future", speech by Cecilia Skingsley, 22 November.

——— (2019): "Payments in Sweden 2019 – the payment market is being digitalised", 7 November.

Sy, A, R Maino, A Massara, H Perez-Saiz and P Sharma (2019): *FinTech in Sub-Saharan African countries – a game changer?*, International Monetary Fund, 14 February, https://www.imf.org/~/media/Files/Publications/DP/2019/English/FTSSACEA.ashx.

Taylor, C, C Wilson, E Holttinen and A Morozova (2020): "Institutional arrangements for fintech regulation and supervision", *FinTech Notes*, no 19/02, International Monetary Fund, January.

Toronto Centre (2018): *SupTech – leveraging technology for better supervision*, July.

Transport for London (TfL) (2020): Contactless and Oyster account.

UK Finance (2018): *Financial inclusion in a digital age*, December.

United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA) FinTech Working Group (2019): *Early lessons on regulatory innovations to enable inclusive FinTech – innovation offices, regulatory sandboxes, and RegTech*, February.

Wechsler, M, L Perlman and N Gurung (2018): *The state of regulatory sandboxes in developing countries*.

White O, A Madgavkar, J Manyika, D Mahajan, J Bughin, M McCarthy and O Sperling (2019): *Digital identification – a key to inclusive growth, McKinsey Global Institute*, April.

Wiebusch, P (2017): *Open banking – a seismic shift*, Deloitte.

World Bank (2014): *Guidelines for the successful regional integration of financial infrastructures*, January.

——— (2016a): *Innovation in electronic payment adoption – the case of small retailers*, June.

——— (2016b): *Universal Financial Access by 2020 – country progress*.

——— (2017): "Leveraging 'suptech' for financial inclusion in Rwanda", 8 June.

——— (2018a): "The global identification challenge – who are the 1 billion people without proof of identity?", 25 April.

——— (2018b): *Technology landscape for digital identification*, February.

——— (2019a): *Identity authentication and verification fees – overview of current practices*, April.

——— (2019b): *Inclusive and trusted digital ID can unlock opportunities for the world's most vulnerable*, 14 August.

——— (2019c): *Mexico – Financial Inclusion Development Policy Financing Project*, May.

——— (2019d): *Global Payment Systems Survey (GPSS)*

World Economic Forum (2015): "How the internet of things will improve banking", 13 May.

——— (2016): "Explainer – the internet of things", 21 July.

——— (2019): "These 5 industries can drive digital financial inclusion", 22 July.

Zhang, L and S Chen (2019): "China's digital economy – opportunities and risks", *IMF Working Papers*, no WP/19/16, January, https://www.imf.org/~/media/Files/Publications/WP/2019/wp1916.ashx.

Zunzunegui, F (2018): "Digitalisation of payment services", *Ibero-American Institute for Law and Finance Working Papers*, no 5/2018.