G20 Policy Guide

Digitisation and informality: harnessing digital financial inclusion for individuals and MSMEs in the informal economy

G20 ARGENTINA PRESIDENCY 2018

g20argentina.com

GPFI Global Partnership for Financial Inclusion

G20 ARGENTINA 2018

BUILDING CONSENSUS FOR FAIR AND SUSTAINABLE DEVELOPMENT

G20 Policy Guide

Digitisation and informality: Harnessing digital financial inclusion for individuals and MSMEs in the informal economy

GPFI Global Partnership for Financial Inclusion

G20 ARGENTINA 2018
BUILDING CONSENSUS FOR FAIR AND SUSTAINABLE DEVELOPMENT

Acknowledgments

The G20 Policy Guide has been prepared on behalf of the G20 Global Partnership for Financial Inclusion. This work builds on the input papers produced by Implementing Partners of the GPFI, namely the Better than Cash Alliance, the Consultative Group to Assist the Poor, the Organisation for Economic Co-operation and Development and the World Bank Group, as well as the International Committee of Credit Reporting. The input papers were developed for each of the GPFI Subgroups, namely the Regulation and Standard Setting Bodies, Markets and Payment System, SME Finance, and Financial Consumer Protection and Financial Literacy. The G20 Policy Guide has also benefited from peer review of representatives from GPFI members pursuant to the consultation process provided by the GPFI Terms of References. Finally, non-G20 countries, facilitated by the Alliance for Financial Inclusion, as well as the Bill and Melinda Gates Foundation, the SME Finance Forum and the UN Secretary-General's Special Advocate for Inclusive Finance for Development provided valuable contributions.

Acronyms

AFI:	Alliance for Financial Inclusion
AML:	Anti-Money Laundering
ARCO:	Access, Rectification, Cancellation, Opposition rights
BTCA:	Better than Cash Alliance
CDD:	Customer Due Diligence
CFT:	Countering Financing Terrorism
CGAP:	Consultative Group to Assist the Poor
CRSP:	Credit Reporting Service Provider
DFI:	Digital Financial Inclusion
DFS:	Digital Financial Services
DFSP:	Digital Financial Service Provider
EU:	European Union
FATF:	Financial Action Task Force
G2P:	Government to Person
GDPR:	General Data Protection Regulation
GPCR:	General Principles of Credit Reporting
GPFI:	Global Partnership for Financial Inclusion
HLP:	High-Level Principles
ICCR:	International Committee on Credit Reporting
ID4D:	Identification for Development
IP:	Implementing Partner
LEI:	Legal Entity Identification
MSME:	Micro Small and Medium Enterprise
OECD:	Organisation for Economic Co-operation and Development (OECD)
P2G:	Person to Government
P2P:	Person to Person
PSD2:	Payment Services Directive
PSP:	Payment Service Provider
QR-Code:	Quick Response Code

Table of contents

Executive summary

Access to and use of financial services plays a critical role in supporting inclusive and sustainable development. Despite remarkable progress in the financial inclusion agenda, large segments of the population remain excluded from the formal financial system. Many financially-excluded individuals and firms are found in the informal economy.

Digitisation offers an unprecedented opportunity to address eligibility and affordability barriers to formal financial inclusion faced by informal individuals and firms. In particular, digitisation can (i) facilitate identity verification, (ii) promote digital payments and (iii) improve the information environment. However, to fulfil its potential digitisation also requires attention to (iv) financial consumer protection and financial literacy.

The G20 Policy Guide presents a set of key policies that support the delivery of interventions to facilitate financial inclusion of individuals and firms operating in the informal economy. It focuses on four key areas that can ease eligibility and affordability barriers.

The following table summarises the key recommendations for each policy area.

Digital on-boarding

Improve the identification and verification of new customers

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

2) Adapt and upgrade the regulatory framework
A conducive regulatory framework should recognise the potential of digital identity

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

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

5) Monitor new developments and approaches to identity
Regulators should keep abreast of technological developments

Digital payments infrastructure

Build an open and inclusive payments ecosystem

1) Prioritise development of interoperable payment systems enabling fast payments
Policymakers should establish a market-based, safe, efficient and interoperable payment system

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

3) Create incentives for consumer use of digital financial services
Use by final consumers should be affordable

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

Use of alternative data for credit reporting	Financial consumer protection, financial literacy, and data protection
Leverage alternative data to enhance credit reporting 1) Improve availability and accuracy of information *The main categories of alternative and reliable data should be identified* 2) Expand credit information sharing *Credit information sharing could be extended to alternative data* 3) Enable responsible cross-border data exchanges *Regional cooperation could help improve consistency and comparability of data* 4) Balance market integrity, innovation and competition *Functional requirements should be applied to ensure quality of treatment*	*Increase opportunities while mitigating risks* Financial Consumer Protection 1) Adapt oversight arrangements and capability for financial consumer protection *Regulators should embrace technology while keeping high standards of consumer protection* 2) Enhance disclosure and transparency *Technology could be leveraged to adapt and strengthen disclosure and transparency standards* Financial Literacy 3) Foster data collection, coordination and identification of new core competencies on digital financial literacy. *New data should be used to identify competency frameworks in a coordinated manner* 4) Strengthen the delivery of financial education for digital financial services and support its evaluation *Digital technology could be leveraged for the provision and evaluation of financial education programmes* Data Protection 5) Enhance secure and effective consent models *Consent models to ensure data protection could be adopted* 6) Enhance access, rectification, cancellation and opposition rights *Consumers should be given options to access and change their own data.* 7) Address data security *Adoption of security measures could help protect against operational risks*

Author: **Moksumul Haque**

Digitisation and informality

Why it is important

Access to and use of financial services plays a critical role in supporting inclusive and sustainable development. Despite remarkable progress in the financial inclusion agenda, approximately 1.7 billion adults worldwide still do not have a basic account at a financial institution or at a mobile money provider.[1] More than half of the unbanked are women, with a gender gap estimated at 7 percentage points globally: whereas 72 percent of men had an account in 2017, only 65 percent of women did so.[2] Although account ownership increased in the past few years to 69 percent, adults reporting formal savings in the past 12 months remained at only 27 percent, while just 11 percent of adults worldwide formally borrowed.[3] Additionally, half of the 400 million micro, small and medium enterprises (MSMEs) in emerging markets lack adequate financing to thrive and grow, with a total credit gap estimated in the range of US$2.1-2.6 trillion.[4] As a result, many individuals and firms have no safe and reliable way to save, invest, make payments and insure against risk. This has negative repercussions for livelihood, productivity, growth and inequality.

Informality represents an important barrier to financial inclusion. For the purpose of the G20 Policy Guide, informality is broadly defined to encompass "all economic activities by workers and economic units that are in law or in practice not covered or insufficiently covered by formal arrangements".[5] While many factors contribute to financial exclusion, individuals and MSMEs operating in the informal economy find it particularly difficult to access and use formal financial services.[6] Around 80 percent of total MSMEs are informal,[7] and these firms consistently report access to finance as the biggest constrain they face.[8] Financial exclusion of both individuals and MSMEs is more widespread in countries where the size of the informal economy is greater.

Figure 1 shows that both account penetration and the share of small firms with a loan from a financial institution are lower in large informal economies, while use of cash and informal borrowing are more widespread when the informal economy represents a larger proportion of the total economy.

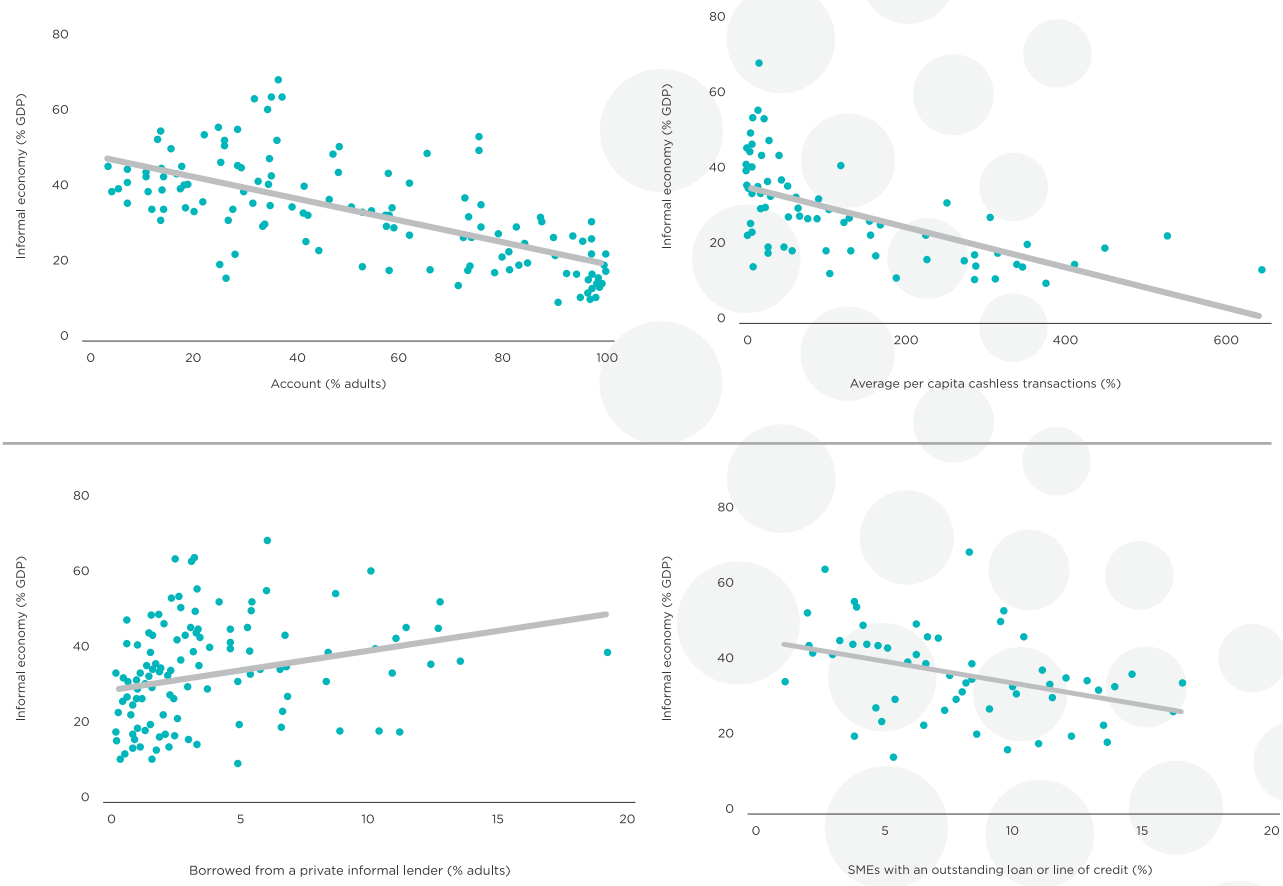
Women constitute the largest group in the informal economy. From street vendors and domestic workers to subsistence farmers and seasonal agricultural workers, women represent the main work force in the informal sector.[9] These women generate their own income and run businesses but often may not have available the benefits of the traditional financial system, lack collateral, credit records and, in the case of migrants, often documentation. Women who work in the informal economy need access to the full range of financial services to generate income, build assets, smooth consumption, and manage risks but these are rarely available to them. This highlights the importance of the gender dimension in the financial inclusion-informality nexus.[10]

Digitisation, or the adoption of digital technologies and approaches, offers a transformational solution to financial exclusion driven by informality. Rapid technological innovation is profoundly reshaping production and consumption of goods and services. One important area where the disruptive impact of new technologies, particularly digital technology, is already visible is financial inclusion. The use of mobile money and digital payments has increased heavily in the past few years, and this might have contributed to the inclusion of more people into the formal financial system.[11] Harnessing digitisation to financially include those in the informal economy and those that have new work arrangements lacking a stable and formal source of income, represents an enormous opportunity.

Digitisation can help address eligibility and affordability barriers, which are among the most salient barriers to financial inclusion faced by individuals and MSMEs operating in the informal economy.[12] Individuals and firms operating in the informal economy are sometimes unable to provide a reliable form of identification that can meet Customer Due Diligence (CDD) requirements to open a bank account. They cannot generally afford using payments services. When applying for a loan, MSMEs in the informal economy have limited collateral and cannot convincingly prove their repayment capacity because of information asymmetries.

FIGURE 1:

Financial exclusion and informality



Source: Medina and Schneider (2017); G20 Global Financial Inclusion Indicators; World Bank Global Payment Systems Survey

To leverage the potential value of digitisation in the informal economy, widespread mobile connectivity and ownership are needed. This is an important precondition for unleashing the opportunities generated by digitisation. To enable broad access to digital financial services, individuals and firms in the informal economy must own a mobile phone and be able to use it wherever they are. Across countries, network coverage is generally high, and phone subscriptions and smartphone ownership are both growing fast. However, certain groups continue to have limited or no access to mobile phones. This is a particular challenge for women who, in most countries, are less likely to own their own phone. Women in low- and middle-income countries are, on average, 14 percent less likely to own a mobile phone than men, with important regional variations.[13] Therefore, it is essential that efforts continue to ensure broad and equal access to mobile technology.

The G20 Policy Guide focuses on how digitisation can help individual and firms operating in the informal economy access financial services to improve their lives or businesses. Digitisation is not a means to formalisation yet access to formal financial services can contribute to reduce informality in the long run. Access to formal financial services can increase the credibility of constrained individuals and firms, helping them overcome the entry cost into the formal sector.[14] It can also boost productivity, reducing the opportunistic informality and the number of individuals and MSMEs that choose to produce and trade in the informal sector.[15] However, informality remains a complex issue that may require policy action on several fronts, including in the areas of institutional development, employment regulations and tax, which are beyond the scope of the G20 Policy Guide.

This document outlines a set of key non-binding policies to financially include individuals and firms in the informal economy. It brings together evidence and consensus-based policy recommendations and guidance on four policy areas. These are deemed important to the fair and affordable inclusion of individuals and MSMEs operating in the informal economy into the formal financial sector (Figure 2). These areas include:

A. Digital on-boarding.
B. Digital payments infrastructure.

C. Use of alternative data for credit reporting.
D. Financial consumer protection, financial literacy, and data protection.

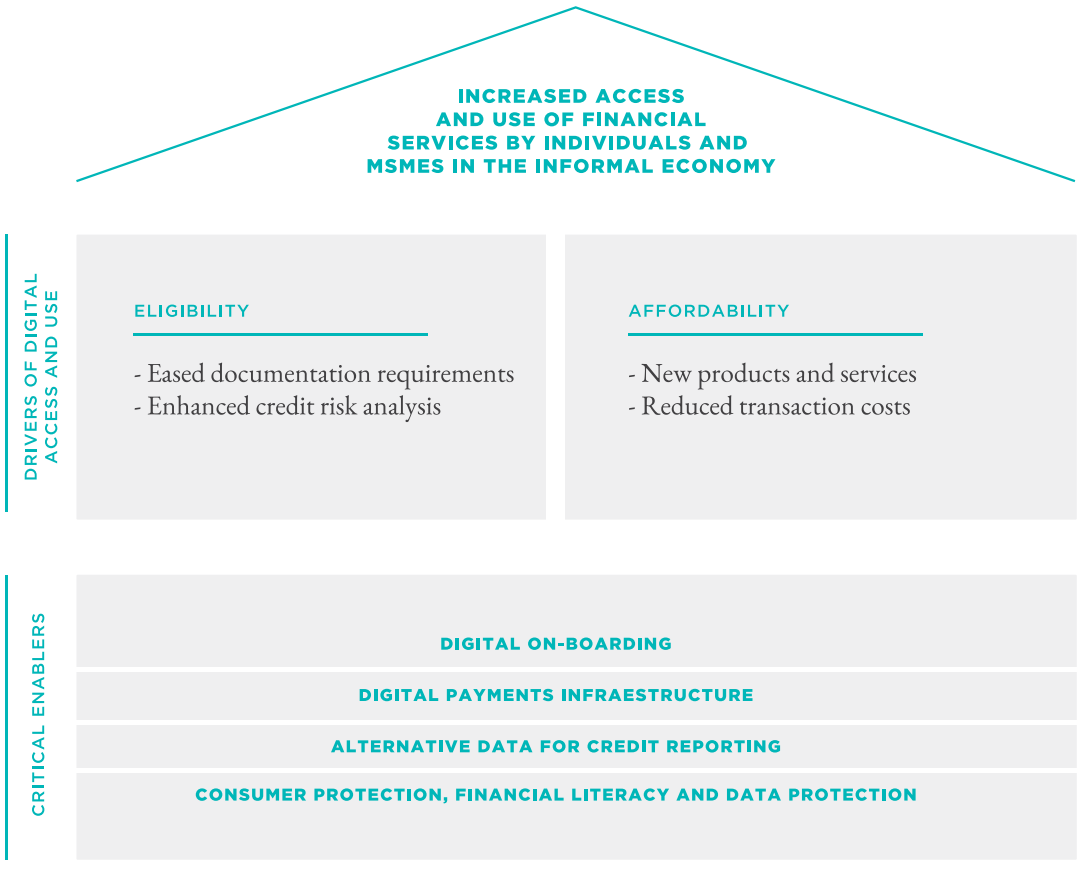
This work is in line with the G20 Financial Inclusion Action Plan and builds upon the work of previous G20 Presidencies, including most recently the G20 Chinese and German Presidencies, and supports the implementation of the G20 High Level Principles for Digital Financial Inclusion (HLP for DFI). The choice of policy areas also reflects technical relevance to address the financially excluded in the informal sector through digitisation. From this perspective, the G20 Policy Guide will contribute to move the GPFI agenda forward by focusing on specific topics that are important in the intersection between informality, financial inclusion and digitisation. However, policy recommendations may change over time, as new evidence on effective interventions is added. For this reason, the G20 Policy Guide should be seen as a living document.

The G20 Policy Guide targets policymakers in both G20 and non-G20 countries who are responsible for developing, implementing and evaluating financial inclusion strategies, plans and programmes, as well as those from sectors that influence financial inclusion outcomes, especially in the informal economy. In addition, a number of actors outside the government may play an important role in delivering digital financial services to the informal sector, including civil society organisations, professional associations and the broad private sector. Concerted efforts by the public and the private sector are therefore critical to capture the opportunity offered by digitisation.

This work aims to support policy dialogue, strategic planning, priority setting and implementation planning. However, the G20 Policy Guide is neither intended to inform nor interpret the work of the global financial sector standard-setting bodies. The G20 Policy Guide suggests key policy measures that could be considered in applicable national financial inclusion strategies and country level actions aiming at financial inclusion, always taking into account country contexts and national circumstances. The G20 Policy Guide includes key building blocks which need not be implemented in sequence, providing flexibility and an opportunity to be used as a check list, if desired. As a result of structural inequality, policy action has different implications for women and men. G20 and non-G20 policymakers and stakeholders are encouraged to undertake systematic analyses of their policies and programs to help eliminate the gender differences that exist in access to finance.

FIGURE 2:

Digitisation and informality



Millions of individuals and small businesses are relegated to the informal economy, getting by without access to the formal financial services they need to protect themselves against setbacks and create opportunities. So addressing informality is a priority in order to expand financial inclusion.

The G20 Policy Guide on Digitisation and Informality is a good start to help us understand how digitisation has the potential to decrease informality. But we must address other elements as well—strengthening financial information infrastructure and data, and developing enabling legal and regulatory frameworks that can provide incentives for formalisation.

I hope that the G20 Policy Guide will lead to more focused research on the contribution that financial inclusion can make specifically on reducing informality, including examples, as well as how informality hinders our progress on financial inclusion.

— H.M. Queen Máxima of the Netherlands, United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA)

Author: **Erin Rufledt**

Digitisation and informality

How to harness opportunities

A. Digital on-boarding[16]

Identification systems play a significant role in enabling financial inclusion. A unique and legal identity is necessary to allow all individuals to participate fully in the society and the economy. Identity verification is also important for MSMEs to establish the identities of the staff and directors authorised to setup, operate and instruct changes for the business. Verification of identity enables service providers to facilitate registration, minimising the risk of fraud and meeting the requirements of CDD regulations.[17] Yet approximately 1 billion people around the world are estimated to lack an officially-recognised proof of identity.[18] This is particularly the case for women and vulnerable groups such as forcibly displaced persons.[19] Where data are available, the female share of the unregistered population often represents more than 50 percent.[20] Progress in the development of identification schemes can therefore positively impact financial inclusion, especially of those individuals and MSMEs operating in the informal economy, given the pervasiveness of eligibility barriers for these segments of the society.

Technology could offer solutions to improve the identification and verification of new customers. The introduction of a digital identification system could potentially lead to more adoption of digital financial services by: a) making it easier for the unbanked to open a transaction account[21] in conjunction with simplifying documentation requirements; b) enabling more cost-effective customer on-boarding that can be conducted remotely; and c) contributing to facilitate the delivery of additional services to the individual. Digital identification systems can also enhance the security credentials and potentially make it a more secure process to enable financial inclusion among people while meeting regulatory requirements of Anti-

Money Laundering/Countering Financing Terrorism (AML/CFT).

The World Bank Principles on Identification for Sustainable Development provide guidance to advance the promotion of robust and inclusive identification systems, in particular digital ones.[22] As Principle 2 highlights, the emergence of new digital approaches, such as biometrics, allows individuals and small businesses to have access to identification services in a more effective way. National and local governments have a primary role in the registration and recognition of legal identity. As stated by Principle 7 of the HLP for DFI, in the financial sector the focus is on legal identity credentials provided by and/or recognised by governments for official purposes.

The legal framework is one of the most important aspects of the identification system, especially when it is scaled up to a variety of functional applications. The need for addressing the lack of identification of individuals and businesses in the legal framework is key to progress on financial inclusion. Approaches to scale up new technologies need to be evaluated, including exploring the role that the private sector can play in building out the digital identification layers. The constant emergence of new technologies and approaches to the identification process should also be monitored closely and policy framework should be adaptive towards these developments in order to take the ecosystem forward.

Based on experience to date and lessons learned from both government identity programs and private sector initiatives, the following policy recommendations are proposed:

1) Ensure an integrated identity framework.
2) Adapt and upgrade the regulatory framework.
3) Establish a robust and secure digital identity infrastructure in the financial sector.
4) Foster development of private sector-led services by leveraging legal identity infrastructure.
5) Monitor new developments and approaches to identity.

1) Ensure an integrated identity framework

A legal or foundational identity system is critical to reliably assign an identity recognised across governments and the private sector. During account opening, a customer is required to provide credentials to establish identity so that the financial service provider can carry out CDD procedures. These credentials then need to be validated and allow the financial service provider to access other sources of information such as credit bureaus to validate the information provided and assess the suitability of the product to the individual. Once complete, a transaction identifier is issued, to conduct the authentication for use in transactions. A legal or foundational identity system forms the legal basis for identity validation for critical services, including for establishing account relationships beyond a specific risk threshold. In the financial sector, once the identity validation is done, the subsequent interactions of the customer with the financial service provider can use other approaches for authentication and authorisation in the process of service delivery.

Policymakers could design a digital infrastructure appropriate for their context, including strategies to reach remote areas and ensure "last mile connectivity." Off-line solutions can complement the absence or loss of on-line connectivity. The development of robust procurement guidelines and open design standards to promote innovation and allow for greater flexibility, efficiency and functionality of the system both within and across borders could be also considered. In addition, the technical capacity of government agencies, private sector and other stakeholders in the digital identity ecosystem (including end-users) to operate and maintain new systems and devices should be ensured.

A biometric-based legal identity system can also potentially support authentication services while complying with AML/CFT regulations, upon which the service provider can further develop authorisation processes. However, wide-spread use of legal identity infrastructure for multiple phases of financial services provision has implications at several levels, including the cost of replacing existing infrastructure established for these processes; the pricing of these services; a liability framework for false-positives and false-negatives for biometric credentials; and the impossibility of replacing authentication credentials in a centralised legal identity database if there is a

compromise of biometric information. Hence, there needs to be careful consideration around using national foundational identity infrastructure for on-going transactional authentication and authorisation, or whether to split the functions and isolate the foundational identity infrastructure from the rest if there exist well-established reliable, efficient and safe processes for these other functions.

2) Adapt and upgrade the regulatory framework

It is important that each country's financial services regulatory framework recognises the potential of digital identity services, and ensures that restrictions on how and where accounts are opened, and who opens them, are calibrated in line with the potential benefits of these technologies. At the same time, any such regulatory reform needs to be done in such a way as to remain aligned with FATF recommendations.

There are many specific areas which may need to be addressed in a conducive regulatory framework. These include (but are not limited to) the following: whether digital identity verification satisfies prevailing AML/CFT requirements; whether legal certainty and equivalence between digital signatures and physical signatures is guaranteed; whether private sector-managed third-party authentication services are recognised as legally equivalent to a bank doing the authentication itself; whether all bank customers should be required to provide a particular type of identity credential, for example one that is considered unique and has digital capabilities; and whether consumer interests are protected when new digital identity services are made mainstream, in particular ensuring that no segment of customers is placed at a disadvantage.

3) Establish a robust and secure digital identity infrastructure in the financial sector

Digital identity systems can introduce new challenges and risks, which need to be addressed by appropriate regulatory and oversight frameworks that apply to both traditionally regulated financial institutions and third parties. Notable risks include data security, which could be mitigated by ensuring robustness of the underlying

technology, systems and processes used for digital identity; protection of privacy; and effective governance arrangements for the use of digital identity infrastructure in the financial sector, particularly as it applies to non-regulated entities.

Identity systems should be vested with security measures to protect the data. Given the nature of the data stored in the systems, security should follow a three-dimensional approach (logical, physical and organisational). It should include not only the system where the data is stored but also the network enabling its access, the back-up systems and any other system linked to the personal data of the individual, including those third parties that perform any task related to the personal data included in the identity system.

4) Foster development of private sector-led services by leveraging legal identity infrastructure

Legal identity infrastructures can provide a foundation on which the private sector can build solutions to meet the needs of the financial sector and beyond. This imposes requirements on the identity platform, in particular on areas of open interfaces and sustainable charging models, but can often allow for more rapid rollout of digital identities than the government may be able to achieve. Two of the Principles on Identification for Sustainable Development specifically call for creating interoperable platforms using open standards for this very reason.[23]

5) Monitor new developments and approaches to identity

There are a number of emerging technologies and new combinations of existing technologies that have the potential to leapfrog a unique national identity platform, digital or traditional. These methods include using distributed ledger technologies and social data. However, these are currently in very early stages of development and do not represent a viable alternative for a comprehensive build out of a foundational legal identity infrastructure. As with any innovation, the capabilities can dramatically increase and hence authorities need to closely monitor developments, use prevalent best practices and think in terms of open interfaces and modular approaches in the build out of legal identity platforms.

Box 1.
CDD requirements and biometrics

The **Reserve Bank of India** has permitted the entities regulated under it to accept Aadhaar identification number issued by the Government of India as proof of identity as well as address to meet the regulatory CDD requirements of opening accounts.

The Aadhaar Digital ID system has been unified with an electronic CDD (e-KYC) service to expedite the verification of a client's identity. The e-KYC enables an individual with an Aadhaar number to allow Unique Identification Authority of India (UIDAI) to disclose his/her personal information to service providers who wish to instantly activate services such as mobile connections and bank accounts.

The e-KYC is paperless, consent-based, private and instantaneous. As a result, accurate and reliable CDD data is shared with the reporting entity in real time. Furthermore, as the KYC data is released directly to service providers only upon the consent of the customer, his/her privacy remains protected. So far, a total of 5.9 billion e-KYC transactions have been completed through Aadhaar.

Banks and payment network operators have embedded Aadhaar authentication into micro-ATMs to provide branch-less banking anywhere in the country in a real-time, scalable and interoperable manner. From the financial services provider's view point, it offers tremendous benefits in terms of near elimination of paperwork and the consequential burden of keeping records and facilitating audit and forensics through the electronic storage of information.

In **Pakistan**, the national ID cards allowed registration of all SIM cards which re-

lied on the extensive agent network built by branchless banking providers. These ID cards enabled the opening of transaction accounts hence growing the branchless banking network.

Biometrics as the name insinuates is the metrics related to human characteristics that are unique and hence used as a means of proving one's identity. There is increasing interest around the world in exploring biometrics for authentication, as a response to (amongst other matters) AML and CFT concerns. Identity services in **India** and **Pakistan** are built on biometrics and **Bangladesh** is expected to follow suit.

Biometrics can be broadly divided into primary iris scans, fingerprints and face recognition and soft biometric- those that are more related to behavioural characteristics and mannerisms. Although they have both been considered for authentication, the former is by far the more prevalent while the latter is often used to understand patterns and trends and hence detect anomalies or unauthorised transactions.

The Payments Association of **South Africa** is working with Mastercard and Visa to design a solution that is interoperable in South Africa. The specification enables a range of biometric solutions, from fingerprint verification to palm, voice, iris, or facial biometrics. However there are concerns that the uptake of this by traders will be low due to the high cost of replacing point-of-sale (PoS) devices.

In 2015 **Nigeria**, began a biometric verification pilot for all civil servants in an effort to get an accurate record of the personnel and ensure 'ghost' salaries were not paid out. The Central Bank of Nigeria required that all customers enrol with their banks to get their unique Bank Verification Numbers (BVN) operated by the Nigeria Inter-Bank Settlement System (NIBSS). In early 2016 they announced the removal of 24,000 workers and that number has since doubled saving the tax payer equivalent of $74million USD.

B. Digital payments infrastructure[24]

Achieving greater access to and use of digital payments is essential for advancing the financial inclusion agenda, especially among individuals and MSMEs operating in the informal economy. The latest data reveal an increased use of digital payments all around the world.[25] Yet a gender gap remains: men are about 5 percent more likely to use digital payments than women.[26] Improving the payments infrastructure could dramatically boost financial inclusion and economic opportunities through increased use of formal payment services.[27] As stated in the HLP for DFI 4 ("Expand the Digital Financial Services Infrastructure Ecosystem"), the development of a payments infrastructure is one of the core enablers for a more inclusive and open digital payments ecosystem.[28]

Many governments recognise that an efficient, widely accessible and open, safe and inclusive digital payments infrastructure is an important enabler for an inclusive and growing economy. By way of general definition, an open payments infrastructure is one that can be accessed by Payment Service Providers (PSP)[29] within the regulated realm. An inclusive payments infrastructure results in payments services that can (ideally) reach any individual or MSME in the country. When the payment infrastructure is both open and inclusive it can drive digital payment volumes. This in turn can reduce unit costs and ultimately end-user fees. It can also enable competition among PSPs, leading to improved products and services and increased usage. But in addition to this, it is essential that individuals and MSMEs have the right incentives to accept those digital payments.[30]

A fully open payments infrastructure might not always be the immediately feasible or desired solution for countries. Joining such an infrastructure might not be viable or possible for some PSPs due to regulatory or financial requirements, e.g., to reduce financial stability risks, or due to existing operational issues. Moreover, some PSPs might abstain from joining the common infrastructure as they fear losing their innovative advantage when for example opening up their closed loop payments system. Those issues, among other specific circumstances like a country's infrastructure

development, have to be considered in moving towards a more open and inclusive payments infrastructure. [31]

From the PSP perspective, progress towards a more open and inclusive payments ecosystem has, in some cases, been impeded by the perceived complexity associated with the participation to the existing payments infrastructures. As mentioned above, new PSPs have often not sought or been granted access to existing payments infrastructure. For example, mobile money was introduced in emerging economies as a way to encourage new classes of transaction account providers to serve unbanked populations. These have generally been introduced as closed loop systems, with limited success beyond domestic person-to-person transfer. The reasons can be found in a combination of factors, including the provider's business case, the cost and difficulty of complying with regulation, and the cost of managing agent networks and liquidity.

From the end-user's perspective, a main challenge to develop a more open and inclusive payments ecosystem has been the lack of interoperability, meaning that the customer of one PSP cannot easily transact or cash-out with a customer of another provider, and a mobile money customer cannot easily interact with a banked person or entity. Another issue, especially relevant for small merchants, has been the valuing of cash over electronic payments due to high cost of acceptance or delayed fund availability as a result of deferred clearing and settlement processes. Therefore, if countries move towards open and inclusive payments infrastructures, it may not only be critical to advance on the interoperability among digital payment services, but also to consider incentives to drive the use of these services vis-à-vis cash, and make formal financial services attractive for merchants and consumers operating in the informal economy. In this regard, utility, cost, security and trust play a major part in end-users' uptake.[32]

The following policy recommendations are intended to help move towards a more open and inclusive payments ecosystem and address the mentioned provider and end-user challenges. Further, recommendations aim to incentivise the system´s use and acceptance among individuals and MSMEs, especially those operating in the informal economy. It goes without saying that an important precondition for the healthy development of a digital payments infrastructure is the establishment of widespread connectivity. Ensuring

a widespread and affordable access to telecommunications networks might need to be encouraged. The main policy recommendations can be summarised as follows[33]:

1) Prioritise development of interoperable payment systems enabling fast payments.
2) Create incentives for merchant payments acceptance.
3) Create incentives for consumer use of digital financial services.
4) Support cross-border payment systems.

1) Prioritise development of interoperable payment systems enabling fast payments

The digital payment systems should allow for interoperability, providing an opportunity to connect all providers to the same system. Many countries have already pushed for their implementation, with the objective of improving efficiency over slow legacy systems and achieving financial inclusion goals. Interoperable digital payment systems need cooperation between all involved stakeholders and can provide lower-cost and lower-risk transactions, enabling greater participation in the payment system and increasing payment efficiencies, thereby contributing to more open and inclusive payment infrastructures. In addition, systems which enable Fast Payments are potentially able to take the adoption of digital payments for everyday use to new levels.

A defining characteristic of a fast payment system is the ability that the transmission of the payment message and the availability of "final" funds to the payee occur in real time or near-real time on as near to a 24-hour and seven-day (24/7) basis as possible, and are considered irrevocable. To achieve this outcome, certain activities associated with clearing have to occur in real time or near-real time and on a continuous basis for each payment order such that delays present in traditional payments do not arise. Settlement of funds between the Payment Service Providers (PSPs), however, does not necessarily need to occur immediately for each and every payment order. Payee funds availability and inter-PSP settlement can be either coupled (i.e. real-time settlement) or decoupled (i.e. deferred settlement).[34]

It may not be practical or feasible in many cases to move from the current reality to a future of ubiquitously available and accessible, interoperable and operationally robust and efficient in a single step. It is therefore important to plan the evolution of

the payment system with a view towards phased implementation. There is no single best-practice route to establish this, but the following design elements should be considered:

• Use of international standards, especially in the exchange of information between systems, including transactional processing.

• The cost to the end-user is crucial. In the early phases this is not a simple matter to determine, but costing should be done on the basis of expected volume rather than short-term cost recovery. It is a matter of positioning the service for long-term benefit for all participants.

• Identify the system´s components that are required and re-use, as far as possible, components already implemented by legacy systems. For example, if the settlement system is structured to handle multiple payment streams, this system could be used for new payment streams as well.

• To establish market acceptance and build trust, promote and secure the implementation of high-volume business cases. The role of payments emanating from government entities and due to such entities (G2P and G2B, as well as P2G and B2G payments) are crucial in this regard.

• Where feasible and where payment service providers do not already utilise a national ID system, it would be beneficial for interested stakeholders to have access to the national ID system in order to ascertain the identity of the real person or legal entity making a payment. This will increase utility and enable informed risk mitigation measures.

• Ensure that all regulated PSPs are able to, either directly or through some form of an aggregator, have access to the payment system. This does not imply that every payment service provider should be granted access, but rather that the criteria for use are based on the risk introduced by the PSP and the technical/operational ability to participate in the system only and does not exclude certain categories of PSPs.

The fast payments systems should be market-based, safe, efficient and low-cost. Participants could collaborate on the infrastructure level, e.g. by creating shared

platforms and making their systems interoperable, and compete through innovation at the services level. This can provide space for competition and innovation while supporting openness and accessibility for providers. Further, this could contribute to levelling the playing field for providers while granting equal access to innovators and users alike. The shared infrastructure approach could ensure concentration of volumes and make "reach" (the ability of any payer to reach any payee) very simple, while keeping transaction costs low and affordable to enhance financial inclusion. At the same time, PSPs should be able to cover on-going costs and make profits.

For fast payments systems to exploit their full potential, settlement systems should be modernised to favour intra-day settlement, and consider real-time settlement and 7x24 hour settlement of transactions. As the number of participants within the payments eco-system increases as does the complexity of risk monitoring, regulators could develop additional capacity and use improved tools, particularly data management and analyses tools, to be able to perform their regulatory responses.

Policymakers could finally consider prioritising the rollout of large-scale use cases, which can demonstrate the utility, safety, and trustworthiness of fast payments systems. Focusing on priority use cases - such as transit, utility bills and marketplace/ street carts - can drive market awareness and volumes. The government itself could consider playing an active role in the payments ecosystem. For example, issuing social benefits or salaries via bulk Government to Person (G2P) payments, could enhance trust in the system, and could quickly drive uptake through its reach into a much larger proportion of households.

2) Create incentives for merchant payments acceptance

Fast payments systems need to be sustainable while investing in innovation, promotion and business development. This requires a robust business model, implying that pricing needs to be viable. At the same time, merchants or other payments acceptors such as billers should not be disincentivised by acceptance fees, while ensuring the commercial sustainability of the fast payment systems. This is particularly true for small businesses and informal retailers. With an acknowledgement that national context vary, policymakers should, where appropriate, consider a variety of incentive measures, including:

• Ensure that there is no "transaction extra charge" levied against Digital Financial Services Providers (DFSPs); such charges are often passed on to merchants and present a significant barrier to acceptance.

• Subsidising the cost of acceptance in the early stages of development. This could be considered by the private sector to reduce the initial cost of acceptance to the merchant and enable wider adoption.

• Consider the use of formal aggregators that connect to a clearing house and are able to group both formal and informal merchants. In this sense, merchants can accept payments regardless of their formalised status, significantly increasing the payment infrastructure.

• Ensure that merchant service providers, when fulfilling regulatory requirements, are given sufficient ability to act on financial and non-financial adjacencies.

• Increase transparency in the market, through the disclosure of exchange fees, discount rates and other commissions.

• Introduce financial incentives such as merchant exemptions, service charge reductions, reduced rates for merchant accounts, or government reimbursement of fees.

• Introduce thresholds for cash payments for a single transaction above which consumer cash payments are not allowed.[35]

• Where appropriate for national taxation schemes and oversight, authorities should consider incentivizing the use of the system for merchant supplier (B2B) transactions by providing tax incentives to merchants who purchase goods and services electronically. However, documentation on the impact of the incentives is scant mainly due to lack of impact evaluation embedded into the interventions and programs.[36]

• Non-financial incentives could be considered, e.g. automated reporting (fiscal, compliance), training and real-time support, etc.

Merchants should also be discouraged from relying on separate business agreements

or technology arrangements with different PSPs in order to accept payments from consumers. Public private partnerships could collaborate with DFSPs on the development of standardised technologies, for example Quick Response codes (QR codes) for merchant payments. Standardisation could support interoperability and improve usability and utility for merchants and customers.

3) Create incentives for consumer use of digital payments

Consumer fees for target use cases should be affordable for underserved populations. Consumer lottery schemes ("will your next bus ticket be free?") can also have an impact on both perceived cost and consumer awareness. For consumer/government interactions, discounts or other incentives for payments made electronically could be introduced. For consumer, financial incentives could include cash rebates, consumer rewards, loyalty programs or government-sponsored lotteries.

As recommended in HLP for DFI on Consumer Protection, it is important to establish clear and uniform regulations around the protection of consumer funds in accounts; the establishment of redress mechanisms, and access to consumer protection information. In addition, as recommended in HLP for DFI 6 on Financial Literacy, it is also important that policymakers consider market education initiatives, particularly with respect to newly implemented faster payments systems. This could be made easier where the providers involved have agreed on a common consumer brand.

4) Support cross-border payments systems

There are a number of initiatives underway or in planning stages to develop payments systems. Some of these are focused on cross-border transactions only, while others have a broader vision of supporting both domestic and cross-border transactions. Authorities in regional blocs are exploring the possibility of using approaches to processing domestic payments transactions, consistent with the principles outlined in the G20 Policy Guide and applicable regulatory frameworks. Cross-border infrastructure may be of benefit in the development of infrastructures used for financial inclusion purposes. Greater volumes through regionalisation of processing could sharply drive down costs, incentivising participation through affordability and ease of use.

Box 2.
Lotteries, loyalty programmes and POS subsidies

In **Mexico**, a 2004 presidential decree established FIMPE, a private trust fund to expand usage of electronic payment channels. Acquirers were free to opt-in and invest in this fund for a joint program to promote POS installation and use of digital payments. FIMPE was funded through acquirer contributions which were returned as fiscal exemptions. The resulting program had two main parts:

i. Demand generation (Boletazo): Lotteries were organized awarding cars to payment card users (more than 3,100 cars were awarded). According to FIMPE, transactions at POS increased 167% from 2003 to 2006 and 1 out of 5 surveyed said they increased their card usage.

ii. Supply generation: Through the trust fund, free POS were installed in merchants who did not have a POS machine and they were also offered a fixed monthly merchant fee up to certain transaction volume. The program also comprised national media campaign targeted to merchants on the benefits of payment card acceptance. According to FIMPE, the POS network increased 96.3% from 2003 to 2006.

According to an IDB report, under FIMPE, 205,000 POS were installed for free to the merchants who usually had to pay 6,000 - 7,000 MXN (approximately US$ 322 – 376). According to Banco de Mexico, POS transactions increased on average by 24 percent per year between 2005 and 2008; and stalled after FIMPE ended rising only 0.2 percent in 2009.

More recently, the Finance Ministry (SHCP) through the program Tablet para el Regimen de Incorporación Fiscal offered a subsidized tablet equipped with mPOS and accounting software for microenterprises registering for tax purposes.

In terms of cash payment caps, starting in 2014, according to article 55 of the Income Tax Law, financial sector institutions must report cash deposits made to taxpayers' accounts when the accumulated monthly amount of cash deposits exceeds 15,000 pesos (approximately US$ 806). Furthermore, Banco de Mexico issued a ceiling for checks payable to the bearer at 5,000 pesos (approximately US$ 268).

The Point-Based Incentive Loyalty Program was an innovation recognized by **Central Bank of Nigeria** (CBN) and Nigeria Inter-bank Settlement System (NISS) Efficiency Awards to "Recognize, Encourage, Reward and Appreciate" financial inclusion-geared innovations of payments industry players. The Points-Based Incentive Program aims to reward consumers for each card transaction conducted at the POS with loyalty "points" which can be accumulated and used to purchase gifts and goods from an online CBN Loyalty Portal.

Author: **Eakarin Ekartchariyawong**

C. Use of alternative data for credit reporting[37]

Around 80 percent of total MSMEs are informal. These firms face a number of challenges that can negatively impact their operations and growth, including limited public infrastructure and weak institutions.[38] However, according to the World Bank Group enterprise surveys, lack of access to finance is consistently reported as the biggest obstacle they face.[39] For self-employed people, and especially women, access to finance can also be an essential pre-condition for their work. For example, only 37 percent of women are able to use their own capital to start up their businesses, compared to 68 percent of men.[40] Informal firms report low use of loans and bank accounts, and a significant majority finance their operations through sources other than financial institutions, including internal funds, moneylenders, family, and friends.[41] Many of these firms would like to become formal (that is, to register), and report that the ease of access to finance would be the most important benefit they could obtain from registering.[42]

Recent evidence indicates that lowering initial registration costs and providing information on registration procedures have only small effects on firm formalisation. Variable costs associated with becoming formal, such as tax payments, may be comparatively more important for informal MSMEs.[43] Unless these firms grow and become sufficiently profitable to cover such costs, it would be difficult for them to enter the formal sector. Enhancing the financial inclusion of informal MSMEs can potentially help them grow and pave their path toward formalisation.[44] Considering that about two-thirds of full-time jobs in developing economies are provided by informal MSMEs, it is essential to step up efforts to improve access to finance for these firms, especially bank credit and other forms of financing.

Lack of credit data is a common cause of financial exclusion for informal MSMEs. Most informal firms do not have accounting systems to record their transactions and generate credible financial statements and projections. Very often, the only standard

information that is available to assess their creditworthiness is the personal credit file or history of the owner of the firm. However, the latter often does not have a formal job and the informal business is the only source of income for her and her family. In this respect, technology can help.

In an increasingly digitised world, vast quantities of "alternative data" are being generated every day, which can complement or substitute for traditional financial data. It is estimated that the world's stock of digital data will double every two years through 2020, fuelled by the phenomenal intersection of and growth in mobile, cloud, big data, and electronic payments.[45] Financial systems are already generating many digitised data that is considered as alternative data. Such information includes online banking transactions, digital payments, and automated utility payments. In some instances, alternative data are being created outside the financial system. Every time MSMEs and their customers use cloud-based services, browse the internet, use their mobile phones, engage in social media, use ecommerce platforms, ship packages, or manage their receivables, payables, and recordkeeping online, they create digital footprints. Data collected through mobile phones and telecommunications (e.g. call data records, airtime top ups, Person to Person (P2P), Government to Person (G2P) and Person to Government (P2G) payment transactions) are also exponentially increasing data trails including for low income consumers in developing and emerging markets.

Traditional and non-traditional lenders have an option to mine this real-time, easy-to-access data, and use it for credit granting decision making. Lenders can use the alternative data to determine capacity and willingness to repay loans. Using alternative data to enhance credit reporting thus represents a large opportunity to expand access to finance to MSMEs, especially those operating in the informal economy. Lenders may leverage alternative data, such as information from utilities or retail lending, behavioural data, online platform and mobile applications to reach new customer segments including MSMEs. Beyond being used to provide access to credit, alternative data may offer valuable granularity on customer preferences and behaviours that can help to design new financial products and services, encourage positive financial behaviours and support the real sector by linking financing to energy, commerce, health or other sectors.

Notwithstanding these benefits, the use of new types of alternative data for financial and other sensitive decisions brings to the fore additional risks. Policymakers face the challenge of striking the right balance between promoting the benefits of the expanded use of alternative data while ensuring adequate data protection and attention to consumer protection, which is addressed in the next section. In this respect, the following policy recommendations are suggested:

1) Improve availability and accuracy of information.
2) Expand credit information sharing.
3) Enable responsible cross-border data exchanges.
4) Balance market integrity, innovation and competition.

1) Improve availability and accuracy of information

A first step would be to identify the main categories of alternative data. Alternative data in the context of credit reporting is information readily available in digitised form that is collected through technological platforms. Two categories of alternative data were identified: structured and unstructured data. The former is "information with a high degree of organisation, such that inclusion in a relational database is seamless and readily searchable by simple, straightforward search-engine algorithms or other search operations." The latter, which can be more useful in the case of first time borrowers, is "information that either does not have a pre-defined data model and/or is not organised in a predefined manner." In both cases, a unique identifier (ID, passport, financial ID, etc.) is necessary to uniquely link the data from all data providers related to the same individual or MSME. In order to improve the availability and accuracy of information, policymakers and regulators could, therefore, evaluate the implementation of unique identifiers such as Passport/ID for individuals, financial numbers that can be generated by regulators or financial institutions, Passport/ID of promoters or for unregistered MSMEs, or company/legal entity registration number for registered MSMEs.

In the case of MSMEs and individuals, policymakers could consider the importance of ensuring efficiency and consistency of national identification systems, where these exist. In countries where they do not exist, focus could be set on alternatives

such as other identification documents issued by public agencies or consider working together with financial regulators to establish national financial identification numbers. For larger and established MSMEs, policymakers and regulators could examine the potential for establishing a Legal Entity Identification (LEI) framework that allows connecting data from different sources to improve accuracy of linked data. Additionally, relevant public-sector agencies in their role as other data sources, specifically to the extent they provide identification services, could therefore analyse the possibility to agree with Credit Reporting Services Providers (CRSP) a way in which the latter can access national ID databases for validation purposes.

Policymakers could also consider addressing data unavailability and poor quality by promoting automation in data collection, processing and ensuring that data is updated; developing and providing access to an open data system and data standards for MSME data, which captures public data such as corporate and financials; and providing guidance on the adoption and use of alternative data, including the circumstances on when structured and unstructured data can be used. Additionally, regulators and policymakers can amend laws and regulations to clarify how alternative data may be processed, taking into consideration data privacy and protection best practices.

The unavailability of data or the poor quality of data represents another impediment for financial inclusion. Governments could also consider digitising government services, such as tax filing, company registration and other government services, to encourage a digital footprint for MSMEs and individuals. Once digitised, consideration should be given to encourage governmental agencies to pro-actively ensure efficient and cost-effective access by CRSPs to datasets they manage, including but not limited to ID datasets, corporate registries, court of law systems data, and property and collateral registries. Therefore, promoting the digitisation of public information is fundamental.

Finally, consideration should be given to promote the use of digital platforms to address the limited footprints of MSME transactions through campaigns and awareness and by offering incentives to credit providers, MSMEs and consumers. Policymakers could encourage MSMEs to use as much as possible digital services

to run their businesses since services that leave a digital record that can be accessed and combined with other information to be analysed for creditworthiness through offering incentive to credit providers, MSMEs and consumers; consumer awareness programmes; and digital financial literacy.

2) Expand credit information sharing

To expand credit information sharing, regulators and policymakers could analyse possible ways of addressing the limited coverage and incomplete data, by promoting open data platforms for CRSPs to interface with other data repository such as court records, company registry, collateral registry and other digitised information. They could make complete information sharing mandatory; expand the scope and list of mandatory data providers to include non-bank financial institutions, e-commerce, and utility companies; reduce or eliminate minimum reporting thresholds; promote information sharing between CRSPs; and open up the credit information sharing market by removing regulatory and financial barriers. Policymakers can assess the feasibility of establishing a Public Credit Registry/Databank when there is inadequate information sharing.

Regulators could also consider the possibility of amending regulations to require all PSPs, including non-bank financial institutions that are not regulated by a financial authority, to report credit data and other relevant information to CRSPs in their jurisdiction. Likewise, the oversight role of authorities such as the central banks over the regulated credit reporting systems and credit bureaus could be elaborated further to accommodate for the use of alternative data for assessing the capability of the MSMEs to get a loan.

Authorities could ensure that laws governing credit information sharing allow CRSPs to be able to offer services to their customers, including retail, corporate and MSMEs. Applicable laws could also allow CRSPs to collaborate, share information and consider joint products to avoid exclusion of MSMEs by CRSPs that usually focus on consumer or corporate lenders, which contributes to financial exclusion. There is a need to reduce or eliminate minimum thresholds for reporting credits/debtors to CRSPs. Additionally, commercial credit information companies and consumer credit

bureaus should be encouraged to seek to collaborate, and to the extent permitted by law, share data among themselves that might be useful to each other and to their respective users. Eventually they could jointly develop certain credit reporting products.

3) Enable responsible cross-border data exchanges

There are no physical borders for most alternative data which are available through platforms that run in the internet and can be accessed from anywhere. However, cross-border data sharing may be hampered by, for example different: data collection; formats; country regulations; retention periods; unique IDs; and dispute handling process. Difficulties may also exist in identifying the source of inaccuracy. To enable responsible cross border data exchanges in the long-run, regulators and policymakers should coordinate and collaborate with relevant bodies to develop cross border data sharing standards and cross border information regulators; harmonise data privacy laws in relation to alternative data; and provide guidance on the processes of cross border sharing of information including the information that can be shared and possibility of evaluating the CRSPs. There is a need for further collaboration at the international level to improve the comparability and consistency of MSME credit data that is shared and eventually used across borders.

Authorities could finally coordinate to improve consistency and comparability of data that is collected and shared and assess the feasibility of implementing the Global Legal Entity Identifier or its variant such as the Identification for Development (ID4D) Initiative by the World Bank Group. There should be an agreement at an international level on a core set of data to be shared across borders on MSMEs covering both financial data and credit performance aspects.

4) Balance market integrity, innovation and competition

Since it is important to preserve market integrity while not unnecessarily inhibiting the access of individuals and businesses to innovative financial services, functional requirement should be consistently applied to ensure equality of treatment. In order to do so, policymakers and regulators could recommend enhanced risk management by CRSPs; increase the rigor and intensity of risk based

assessments to operations to CRSPs; and collaborate on the development of principles of responsible innovation. To deal with the opaqueness over the use of alternative data, authorities should encourage transparency and disclosure of scoring methodologies of CRSPs that use alternative data. Authorities could also push for or participate in global surveys or similar tools performed periodically to obtain detailed, comprehensive and systematic information about credit reporting activities both in their jurisdictions and at the global level. Likewise, policymakers and regulators could consider the feasibility of implementing or utilising regulatory tools for enabling innovation to promote alternative data centric innovations, including alternative scoring techniques, in their own specific markets.

Box 3.
Global Legal Entity Identifier, open data system and APEC crossborder credit information sharing

The **Legal Entity Identifier (LEI)** is a 20-digit, alpha-numeric code based on the ISO 17442 standard to uniquely identify distinct entities that engage in financial transactions in the broadest definition. It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. Simply put, the publicly available LEI data pool can be regarded as a global directory, which greatly enhances transparency in the global marketplace. The publicly available LEI data pool is a unique key to standardised information on legal entities globally. The data is registered and regularly verified according to protocols and procedures established by the LEI Regulatory Oversight Committee. In cooperation with its partners in the Global LEI System, the Global Legal Entity Identifier Foundation (GLEIF) continues to focus on further optimising the quality, reliability and usability of LEI data, empowering market participants to benefit from the wealth of information available with the LEI population.

Open data systems are platforms where some data is freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control. Open data systems can either be private or government initiated. Some examples of open-data initiatives include **Data.gov, Data.gov.uk and Data.gov.in and open banking** (when banking data is shared be-

tween two or more unaffiliated parties, through APIs, to deliver enhanced capabilities to the marketplace).

Open banking is one of the drivers behind the **EU's revised Payment Service Directive (PSD2)**, which requires Financial institutions In the E.U. to release customer data to authorised third parties using open and standardised applied programming interfaces (APIs).A potential implication of open APIs could be the use of data and liquidity information to provide a very dynamic view of creditworthiness upon the client's specific consent. Some providers, such as bonify.de in Germany, are using transactional data (debit and credit movements on accounts, liquidity levels and historical changes) to create a creditworthiness score which is quite different from the static approach of the past. Instead of looking at long term statistical means they maintain an always up-to-date score based on both historical and current transactional data.

The International Finance Corporation and the Business Information Industry Association were invited by **Asia Pacific Economic Cooperation (APEC)** Business Advisory Council to conduct a pilot on the cross-border access of MSME credit information involving some CRSPs from five jurisdictions, Thailand, Cambodia, Lao, Vietnam and China, as part of the implementation of the credit information system elements of the APEC Financial Infrastructure Development Network (FIND). Efforts are currently underway to create a regional data dictionary to enable easier interpretation of cross border credit reports. These efforts will also include identification of any data elements (such as gender) that might be prohibited from being reported within a particular jurisdiction but which are commonly reported in other jurisdictions.

Author: **Beuttah**

D. Financial consumer protection, financial literacy, and data protection[47]

Digitisation can create opportunities to develop financial literacy competencies, confidence and experience with finance. The use of consumer and entrepreneurs' data, potentially including big data, by financial services providers can generate insights into individuals' spending habits, facilitating the offer of tailored products and supporting fraud detection. Under the appropriate data protection framework, these benefits can be substantial for consumers and entrepreneurs worldwide. They could also open up opportunities to integrate the low income and financially excluded groups in the formal financial sector by creating alternative indicators of behaviour that can be used to assess their risk as customers. For example, gender differences in financial literacy worldwide exist, with women 5 percent less literate than men, and technology offers an opportunity to close this gap.[48]

Digital technology can increase opportunities for fruitful interactions between financial services providers and consumers through digital interfaces. Such interactions can take advantage of behavioural insights, enhancing consumer and entrepreneurs' understanding of financial products and financial decisions. It can also contribute to broadening the range of providers. The digital revolution goes hand-in-hand with new providers entering the market and offering financial services directly to individuals through digital channels. These fintech companies, usually focusing on one product or service, can have an impact on the level of competition in the financial markets and contribute to lower costs, and offer improved experience to individuals and entrepreneurs.

At the same time, digitisation carries new risks for financial consumers. These risks can be:

• Market driven: this can include misuse of unfamiliar (or new types of) products or to uninformed consumers; new types of fraud, often taking advantage of consumers uncertainty in the digital environment; a lack of security, privacy and

confidentiality of data; inappropriate or excessive use of digital profiling to identify potential customers and exclude unwanted groups; rapid access to high-cost/short-term credit or essentially speculative products (e.g. initial coin offerings), and other market practices that can reinforce behavioural biases.

• Regulation and supervision driven: this can encompass uneven levels of protection within (inadequate disclosure and redress mechanisms) and across countries (variety of providers, crossborder selling, regulatory arbitrage); consideration of data protection issues; a lack of coordination among authorities, for example with respect to new types of digital financial services.

• Consumer driven: the growing digitalisation of daily life and of financial decisions is not necessarily matched by increasing digital and financial literacy levels[48], and this is true even among the younger population.[49]

• Technology driven: the increasing use of algorithms, which 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; misuse of data including big data and small data; unreliability of mobile networks and digital finance platforms may lead to inability to carry out transactions; inaccessibility of funds or cybersecurity risks.

These risks can have a negative impact on consumers, and can result in a range of negative outcomes. They can perpetuate lack of, or uneven level of, trust in digital financial services, the financial system and technological innovation. Security measures must be ensured by financial providers to avoid fraudulent transactions and other security risks. Consumers should adopt security precautions when using digital channels. New types of exclusion for certain groups of the population (possibly including the elderly, women and entrepreneurs) can arise as a result of the use of big data and digital profiling for credit and insurance decisions. Low levels of financial and digital literacy and a lack of familiarity with the products available and new providers can increase self-exclusion. Finally, other unintended consequences such as over-indebtedness can surface, especially if consumers, particularly those who may be vulnerable, are tempted by immediate credit offers that play on preferences for instant gratification, or high-cost credit with limited checks on affordability are granted without proper monitoring

(possibly including young people and students in particular, and low-income segments with limited access to more affordable credit).

Maximising the opportunities offered by digitisation requires a better understanding of consumers' behaviours and attitudes towards digital financial services, as well as of the financial and digital literacy needs and demands resulting from technological uptake. A sound financial consumer and data protection framework and increased digital and financial literacy are essential to the responsible and beneficial development of digitisation. Building trust and confidence in the acquisition and use of digital financial services for the financially excluded requires that regulation both promote innovation and incorporate financial consumer protection. In this sense, policies and approaches need to evolve and adapt in line with the environment.

In this context, the following policy recommendations are proposed:

Financial consumer protection

1) Adapt oversight arrangements and capability for financial consumer protection.
2) Enhance disclosure and transparency.

Financial literacy

3) Foster data collection, coordination and identification of new core competencies on digital financial literacy
4) Strengthen the delivery of financial education for DFS and support its evaluation.

Data protection

5) Enhance secure and effective consent models.
6) Enhance access, rectification, cancellation and opposition (ARCO) rights
7) Address data security.

Financial consumer protection

1) Adapt oversight arrangements and capability for financial consumer protection.

It is important to achieve the right balance between allowing technological innovations without undue limitations and ensuring that an appropriate level of financial consumer protection is maintained. Oversight arrangements and capability relates to the powers, structures and capabilities of the legal and institutional arrangements required to supervise and enforce financial consumer protection regimes. Technological developments present a range of challenges and opportunities for domestic public authorities responsible for the oversight of financial consumer protection, including balancing the development of fintech innovations while ensuring the appropriate level of consumer protection; and ensuring the adequacy of supervisory tools, resources and capabilities to oversee digital financial services.

Oversight bodies should ensure they have adequate knowledge of the financial services market, including by engaging with businesses, industry representatives and consumers to understand new digital products and services and identify market trends and issues. Oversight bodies should also ensure that regulatory and supervisory resources, tools and methods are appropriate and adapted to the digital environment, which includes having access to data and exploring the use of technology to assist in market supervision.

Oversight bodies should also be capable of dealing effectively with technological innovation issues while ensuring appropriate consumer protections are maintained. Depending on the circumstances, approaches may include establishing mechanisms such as "regulatory sandboxes" to allow new business models to be tested in a controlled environment, applying proportionate regulatory requirements and providing regulatory support, advice or guidance on the application of the regulatory framework.

Cross-border cooperation aimed at ensuring that financial consumers

remain protected through digital channels could facilitate cross-border transactions, contributing to promote consistency, reducing opportunities for regulatory arbitrage and supporting enforcement activity. This could be done through information sharing among oversight bodies from different jurisdictions. Given the provision of financial services through digital channels can facilitate cross-border transactions which can present particular risks, oversight bodies from different jurisdictions should cooperate, for example to support effective complaints handling or enforcement activity, to ensure consumers remain adequately protected.

2) Enhance disclosure and transparency

Requirements relating to disclosure and transparency are a fundamental part of most financial consumer protection regimes. Technological developments, including the availability of data, provides opportunities to improve disclosure approaches based on a better understanding of consumer decision-making (and an increasing recognition of the limitations of disclosure by itself) and to explore alternatives.

Approaches for consideration by policymakers include, *inter alia*:

- Evaluating existing disclosure requirements in the context of digital financial services to ensure they take account of disclosure via digital means.

- Embedding an understanding of consumer decision-making and the impact of behavioural biases to ensure a consumer centric approach.

- Encouraging financial services providers to test digital disclosure approaches to ensure their effectiveness, taking into account factors such as different screen sizes, communication formats, different local languages and dialects and the digital literacy of the target audience for the product.

Technological developments and the increasing availability of big data also have the potential to create opportunities to explore alternatives to traditional

forms of disclosure, for example, the publication of particular indicators relating to a financial product or service (e.g. consumer complaints) useful in decision-making, "smart defaults" where consumers are defaulted to the a particular option; or "personalised friction" which allows consumers to create steps which act as breaks in a financial transaction. In relation to the provision of advice, including digital advice, approaches for consideration by policymakers include ensuring that algorithms underlying the generation of digital advice are objective and consistent, and that the methodology underpinning digital advice services is clear and transparent, including options for recourse.

Financial literacy

3) Foster data collection, coordination and identification of new core competencies on digital financial literacy

Policymakers should as a priority collect and analyse data on the impact of digital financial services on consumers and entrepreneurs and identify key indicators both on the supply and demand side. On the supply side, data collection should focus on the products and services available, the distribution channels used by providers, and if relevant, the physical infrastructure required for a safe development of DFS and the technological requirements that enable it; on the demand side, policymakers should investigate the demand for and use of DFS, as well as the attitudes, behaviours, the digital and financial literacy of the population. This should also be instrumental in identifying the target groups that are most in need of specific financial education interventions.

In laying the groundwork for the development of these initiatives, policymakers should also ensure coordination with private and not-for-profit stakeholders involved in financial literacy and innovation, in a way that avoids conflicts of interest. This should begin with a mapping of the actors involved in the provision of DFS and of their online platforms and tools, with a view to understanding the

message conveyed and possible risks for unaware consumers. It should also entail the involvement of relevant actors, those with expertise and carrying messages that are consistent with those of policy makers, in the design and development of digital financial literacy initiatives.

Policymakers should draw on available data and research to develop or fine-tune core competencies frameworks for the target groups identified, and develop appropriate financial education content. Building on existing core competencies frameworks on financial literacy, such as those developed at the international level, public authorities should consider additional core competencies required for a safe and beneficial use of DFS[50] that can contribute to:

- Build trust and promote beneficial use of DFS and related technological innovation.
- Protect consumers and small businesses from vulnerability to digital crime and misuse/mis-selling.
- Empower consumers to counter new types of exclusion due to the potential misuse of data sources, including data analytics and digital profiling.
- Support consumers at risk of over-reliance on easy access to online sources of credit.

4) Strengthen the delivery of financial education for DFS and support its evaluation

Based on these core competencies, the authorities responsible for financial education, in cooperation with relevant stakeholders, should support the effective delivery of financial education through digital and traditional means and address the needs of target audiences through tailored approaches. This should be undertaken in particular exploiting the advantages of digital delivery. Digital tools can first improve access to financial education by:

- Making it more affordable and accessible by wider audiences.

• Making it more palatable for all given the opportunity to depict information in a flexible, dynamic and graphic way more easily adapted to the target audience.

• Tailoring financial education to individual needs, through the possibility of setting up profiles or accounts on digital platforms and obtaining personalised information, instruction and advice.

Digital tools can also help reinforce core competencies, confidence and experience with DFS as they can allow to test financial concepts and products in real time, learn by trial and error, and experience failure in a controlled (and artificial) environment, thereby help shaping consumers' habits and attitudes to finance and strengthening the overall financial decision-making process. This can enhance money management skills and control over finances, and help to address consumers' personal biases, while incentivising positive financial behaviours through personal goal setting, feedback mechanisms and reminders. Policymakers should also consider that specific vulnerable target groups or entrepreneurs may still benefit from more traditional delivery tools, such as workshops, and that the needs of young people can be first and foremost met through the inclusion of financial education for DFS in the school curriculum.

Data protection

Policymakers should promote and support the evaluation of the impact and effectiveness of both financial education programmes addressing DFS and the digital tools chosen to achieve financial education outcomes. Consideration should be made to applying a standard framework for evaluation and reporting, to facilitate the comparison of results and to encourage further research on the data if possible. Ideally, such a framework will draw from existing tools developed at the international level.

5) Enhance secure and effective consent models

Consent is a fundamental principle concerning data privacy and financial

consumer protection. Policymakers should enhance consent models and adopt—whenever necessary—mechanisms that are meaningful and pragmatic. Given the intrinsic limitations in the consent model, alternatives to the need for effective and informed consent, and innovative ways to obtain consent, should be implemented.

Regulators could encourage industry participants to adopt a "privacy by design" approach. Put simply, this concept envisages building privacy into all stages of the design and architecture of information systems, business processes, and networked infrastructure. The focus is on taking a proactive, preventive approach to the protection of privacy and the avoidance of privacy harms.[51] The concept rests on the following seven principles: (i) Proactive, not reactive; preventive, not remedial; (ii) Privacy as the default setting; (iii) Privacy embedded into design; (iv) Full functionality—positive-sum, not zero-sum; (v) End-to-end security—full life-cycle protection; (vi) Visibility and transparency—keep it open; and (vii) Respect for user privacy—keep it user-centric. This approach could be implemented through the adoption of a consent management system which would also allow for granularity of the choice to be made by consumers.

Minimisation of data collection should be considered. Regulators could identify key data items that are relevant for risk evaluation, identify those data items that should only be captured and used under specific circumstances or allow industry participants to evidence the relevancy of such data to the purpose of risk evaluation. This concept envisions that only the minimal amount of data should be collected. As an example, the General Data Protection Regulation (GDPR) covers this principle under its Article 5(1)(c), which states: "Personal data shall be... adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')." In addition, the General Principles of Credit Reporting (GPCR) under GP1 establishes that "data collected should include all relevant information to enable any given user to adequately evaluate and manage credit risks on a continuous basis". The GPCR establishes a limit on the data that can be shared which is associated with the permissible purposes underlying information sharing or privacy considerations when dealing with sensitive issues such as ethno-demographic data".

It may be appropriate to introduce a concept of tiered consent by which consumers will be required to give different types of consent for the processing of certain types of data or for specific purposes. When adopting a consent model that enables consumers to decide the type of data that they choose to share and the service providers that they allow to access their information, regulators should bear in mind that there are certain circumstances and data items that do not allow for consent (e.g. us of default data on credit repayment). The adoption of a "privacy by design" approach would facilitate the choice of consumers regarding this layered consent.

A further alternative could be an expiry date for consents. Given that consents are virtually never reviewed or renewed, there should be a limitation period on the effectiveness of some forms of consent. It is, however, acknowledged that such an approach would not solve all the issues with informed consents. In the case of traditional data used to evaluate risk (i.e. credit repayment data) this solution might not apply at least until the obligation is fully performed.

Opt-in as opposed to opt-out consent could be a preferred option for regulators. For instance, the recitals to the GDPR state that "silence, pre-ticked boxes or inactivity should not [...] constitute consent." Industry participants could enable this feature by including clear processes to ensure that consumers receive all the relevant information to make their choice. Technological features and consent management systems could facilitate this process.

Industry participants (and data sources) should be responsible to record evidence of consent being collected from consumers. This is even more relevant when data is to be shared with third parties. For this process a consent management system would be useful. While many consumers care about giving meaningful consent, they often provide it without reading the terms and conditions of their consent. To address these issues, consideration could be given to developing tools that provide for simpler, more clearly expressed, and highlighted forms of consent. Such tools could well be technology-based. They could include a requirement for the use of standardised forms of consent, as well as the option of having verbal forms of consent that would be recorded by the

financial services provider.

Policymakers and industry participants could adopt measures to ensure that the predictive ability of alternative data is tested and verified, that data is used fairly and scoring models developed using alternative data are neutral to minorities or protected groups. Consent is required when sensitive data (e.g. race, ethnic origin, sexual inclination, political or religious affiliation) is used in the evaluation of consumers' creditworthiness and when data included in the model is collected for a different non-compatible purpose. The use of alternative data that carries forward historical discrimination could either be prohibited or restricted, taking into account its ability to predict risk and the availability of alternative decision-making tools.

6) Enhance access, rectification, cancellation and opposition (ARCO) rights

ARCO rights are especially relevant in a digital financial services' context when an individual's data is held, or can be accessed, by multiple institutions and the data may be in many different forms. Consumers may not know who is holding, or has access to, their data, for what purpose it is being used, where it is being held or by whom, or the nature and scope of the data that is being held

At the minimum, allowing consumers to access their own data is a broadly accepted principle and practiced in countries where a data protection law is in place. It is also practiced in those countries where there is no data protection law but there are industries that collect, process and distribute data as part of their core business. Timeline to enable the access ranges from 1-7 days.

Consumers should be given options to correct their data. There is typically a timeline between the request by the consumer to the final resolution by the data controller. This timeline ranges from 7-25 days. However, for the use of alternative data from open sources as opposed to closed networks it is important to highlight the need to identify the data source and the person responsible for the accuracy of data as such person would also be the responsible to correct such data and respond to the consumer. The right to cancel (erase) data is linked to the right to be forgotten, the obsolescence of data and the usefulness

of such data. In closed networks information is typically kept for a determined amount of time and consumers are also able to request the erasure of data when such data is not lawfully collected or has no legal grounds for its further processing.

Consumers should be given the right to make decisions regarding the use of their information for certain purposes. This is typically the case of such use as for marketing related purposes through the introduction of white lists for example. However, there are certain types of data and circumstances where the consumer cannot object the processing of such data (i.e. credit repayment data for credit risk evaluation when such repayment is in default). In closed networks there are certain data items considered mandatory and therefore not subject to this consumers choice. In open networks, the choice of consumers regarding the further use of data is broader.

7) Address data security

Data is becoming a key asset and personal data and identity theft become a major risk for consumers. Internationally agreed frameworks capture the need for safeguards to protect data against unauthorised access, loss, destruction, manipulation and data corruption. In this regard, policymakers should encourage the adoption of security measures to avoid data loss, corruption, destruction, unauthorised access, manipulation or misuse of such data and conduct cybersecurity risk assessments to also strengthen information technology systems, identifying potential threats, enabling mitigating measures and setting up prompt response to incidents would contribute to minimise the consequences of a cyber-incident. Policymakers could also set out rules and mechanisms enabling and encouraging reporting of incidents of criminal nature to law enforcement authorities and information exchange between public and private entities.

Regulators could encourage financial services providers the adoption of security measures to avoid data loss, corruption, destruction, unauthorized access, manipulation or misuse of such data. These measures could also include agreed protocols for incident response including the communication of data breaches. While the timeline for such communication varies from one country to another.

Cybersecurity assessments should be part of the overall risk management policies and

procedures of any service provider or data provider. In this context, identifying potential threats, enabling mitigating measures and setting up prompt response to incidents would contribute to minimise the consequences of a cyber-incident. Ideally, organisations should identify a person to act as Data Security Officer (DSO).

Authorities should continue to seek to leverage the benefits of cross-border data flows. All data flows –domestic and cross-border- should have mechanisms to ensure accountability of data controllers and industry participants and should put in place procedures and policies to allow consumers implement their rights regardless where the data is stored or has been transferred. Finally, cooperation agreements between authorities could facilitate achieving mutual objectives, including with respect to ensuring consistency with AML and privacy frameworks.

Box 4.
Advice provided to new entrants and innovation hubs

The **United Kingdom Financial Conduct Authority** operates an Advice Unit, which provides regulatory feedback, including individual guidance, informal steers and signposting to existing rules/guidance to firms developing automated models of lower cost financial advice to consumers.

The **Japan Financial Services Agency** supports fintech firms through a Fintech Support Desk and a FinTech PoC (proof of concept) Hub. The FinTech Support Desk responds to inquiries, mainly on the interpretation of the law, within 5 working days on average to address the concerns of fintech firms. The FinTech PoC Hub offers a venue for conducting trials with other relevant authorities, by forming special working teams within the FSA for each selected PoC project.

The **Bank of Italy** has recently launched its innovation hub (Fintech Channel), a dedicated space on its web site where operators propose projects with innovative features. The aim is to open up a channel of dialogue with operators and to support innovation processes.

Notes

[1] Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S. and Hess, J. (2018). The Global Findex Database 2017: Measuring Financial Inclusion and The Fintech Revolution. Washington DC: The World Bank Group.

[2] World Bank Group (2018). The Little Data Book on Financial Inclusion. Washington DC: The World Bank Group.

[3] Ibid.

[4] International Finance Corporation (2017). Alternative Data Transforming SME Finance. Washington DC: IFC.

[5] See International Labor Organisation (2013). Decent Work and the Informal Economy. Geneve: United Nations. See also ILO's 2002 International Labour Conference Resolution and Conclusions concerning decent work and the informal economy.

[6] International Labor Organisation (2014). Transitioning from the Informal to the Formal Economy. Geneve: United Nations.

[7] MSME Finance Gap Database. Washington DC: The World Bank Group.

[8] World Bank Enterprise Surveys (various years).

[9] International Labor Organisation (2014). Women and Men in the Informal Economy: A Statistical Picture. Geneve: United Nations.

[10] Promoting financial inclusion of women in the informal economy requires improvement in the quality of disaggregated data. See Co-Chairs' Summary of the Joint Development and Finance Ministers' Meeting of the G7 held in Canada on June 1st, 2018. See also Women Financial Inclusion Data Partnership (2018). The Way Forward: How Data Can Proper Full Financial Inclusion For Women.

[11] ibid.

[12] While physical access and connectivity are important barriers to financial inclusion, recent evidence points to the important role played by eligibility and affordability in the informal sector. See, for example, Honohan, P. and M. King (2012). Cause and Effect of Financial Access: Cross-country Evidence from the Finscope Surveys, in R. Cull, A. Demirguc-Kunt, and J. Morduch (eds.), Banking the World: Empirical Foundations of Financial Inclusion. MIT Press, Cambridge; King, M. (2012). The Unbanked Four-fifths: Informality and Barriers to Financial Services in Nigeria. IIIS Working Paper 411.

[13] GSMA (2018). The Mobile Gender Gap Report. February 2018.

[14] See Capasso, S. and T. Jappelli (2013). Financial Development and the Underground Economy. Journal of Development Economics, 101(C): 167-178.

[15] Beck, T. and M. Hoseini (2014). Informality and Access to Finance: Evidence from India. Centre Discussion Paper Series No. 2014-052.

[16] This section builds upon the input paper prepared by The World Bank: "G20 Digital Identity Onboarding Paper". Washington DC, 2018.

[17] CDD standards are set forth in the Recommendations of the Financial Action Task Force (FATF), the principal stan-

dard-setting body for preventing money laundering and terror financing. The G20 Policy Guide does not purport to interpret the FATF Recommendations or to summarise relevant FATF guidance.

[18] World Bank Identification for Development (ID4D) dataset.

[19] Global Partnership for Financial Inclusion (2017): GPFI Policy Paper – Financial Inclusion of Forcibly Displaced Persons.

[20] Ibid.

[21] 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. See Committee on Payments and Market Infrastructures and World Bank Group (2016). Payment aspects of financial inclusion. Bank for International Settlements and World Bank Group, 2016.

[22] World Bank Group (2017). Principles on Identification for Sustainable Development: Toward the Digital Age. Washington DC: The World Bank Group.

23 Ibid.

[24] This section builds upon the input paper prepared by Better than Cash Alliance (2018): "Achieving Development and Acceptance of an Open and Inclusive Digital Payments Infrastructure. A Guidance Note for the G20/GPFI Markets and Payment Systems Subgroup". New York, 2018.

[25] World Bank Group (2018): The Little Data Book on Financial Inclusion. Washington DC: The World Bank Group.

[26] Demirgüç-Kunt et al. (2018), op. cit.

[27] When the Mexican government digitised and centralised payments, the cost to distribute wages, pensions, and social welfare dropped by 3.3 percent—or nearly US $1.27 billion. See Better than Cash Alliance (2013). Sustained Effort, Saving Billions: Lessons from the Mexican Government's Shift to Electronic Payments. New York.

[28] Global Partnership for Financial Inclusion (2016). Guidance Note on Building Inclusive Digital Payments Ecosystems.

[29] A payment service provider is an entity that provides payment services, including remittances. Payment service providers include banks and other deposit-taking institutions, as well as specialised entities such as money transfer operators and e-money issuers. See Committee on Payments and Market Infrastructures and World Bank Group (2016), op. cit.

[30] Better than Cash Alliance (2018), op. cit.

[31] Committee on Payments and Market Infrastructures and World Bank Group (2016), op. cit.; CPMI (2014). Non-Banks in Retail Payments. Bank for International Settlements; and International Telecommunication Union (2016). ITU-T Focus Group Digital Financial Services. Access to Payment Infrastructures. Geneve.

[32] World Bank Group and World Economic Forum (2016). Innovation in Electronic Payment Adoption: The Case of Small Retailers. Washington DC.; and BTCA (2018), op. cit.

[33] Better than Cash Alliance (2018), op. cit.

[34] Committee on Payments and Market Infrastructures (2016). Fast Payments – Enhancing the Speed and Availability of Retail Payments. Bank for International Settlements.

[35] Ernst & Young and Master Card (2017). Reducing the Shadow Economy through Electronic Payments.

[36] World Bank Group (2016). Supporting Payment Sector Development: B2B Corporate Payments Requirements in the Traditional Retail Sector". Washington DC: The World Bank Group.

[37] This section builds upon the input paper prepared by the International Committee on Credit Reporting and Global Partnership for Financial Inclusion: "Policy Guidance Note on the Use of Alternative Data to Enhance Credit Reporting". Washington DC, 2018.

[38] MSME Finance Gap Database. Washington DC: The World Bank Group.

[39] World Bank Enterprise Surveys.

[40] UN Women (2015). Progress of the World's Women 2015–2016: Transforming Economies, Realizing Rights. New York: United Nations.

[41] Farazi, S. (2014). Informal firms and financial inclusion: Status and determinants. Policy Research Working Paper No. 6778. Washington, DC: The World Bank Group.

[42] Ibid.

[43] Bruhn, M. (2013). A Tale of Two Species: Revisiting the Effect of Registration Reform on Informal Business Owners in Mexico. Journal of Development Economics (103): 275–83.; de Andrade, G., M. Bruhn and D. McKenzie (2013). A Helping Hand or the Long Arm of the Law? Experimental Evidence on What Governments Can Do to Formalize Firms. Policy Research Working Paper 6435. Washington, DC: The World Bank Group; De Giorgi, G. and A. Rahman (2013). SME's Registration: Evidence from an RCT in Bangladesh. Economics Letters 120 (3): 573–78; Campos, F., M. Goldstein and D. McKenzie (2013). Business Registration Impact Evaluation in Malawi. Unpublished paper. Washington, DC: The World Bank Group.

[44] Ibid.

[45] Global Partnership for Financial Inclusion and International Finance Corporation (2017). Alternative data transforming SME finance. Washington, DC.

[46] This section builds upon the input paper prepared by the Organisation for Economic Co-operation and Development through the G20 OECD Task Force on Financial Consumer Protection: "Policy Guidance Note – Financial Consumer Protection Approaches in the Digital Age". Paris, 2018, for the Consumer Protection sub-section; the Organisation for Economic Co-operation and Development through OECD International Network on Financial Education: "Policy Guidance Note on Digitalization and Financial Literacy". Paris, 2018, for the Financial Literacy sub-section; and The World Bank and Consultative Group to Assist the Poor: "Data Protection and Privacy for Alternative Data". Washington DC, 2018, for the Data Protection sub-section.

[47] Hasler, A. and A. Lusardi (2018). The Gender Gap in Financial Literacy: A Global Perspective. Global Financial Literacy Excellence Center. The George Washington University School of Business.

[48] See OECD/INFE (2016). International Survey of Adult Financial Literacy Competencies. Paris: OECD; G20/OECD INFE (2017). Report On Adult Financial Literacy in G20 Countries. Paris: OECD.

[49] See OECD (2014). PISA 2012 Results: Students and Money: Financial Literacy Skills for the 21st Century (Volume VI). Paris: PISA, OECD Publishing; OECD (2017). PISA 2015 Results: Students' Financial Literacy (Volume IV). Paris: PISA, OECD Publishing.

[50] For further details see OECD/INFE Policy Guidance Note on Digitalisation and Financial Literacy. Paris: OECD.

[51] See, for example, Deutsche Gesellschaft für Internationale Zusammenarbeit (2017). Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion. Bonn: Germany.