WORLD ECONOMIC FORUM

Connecting Digital Economies: Policy Recommendations for Cross-Border Payments

INSIGHT REPORT

JUNE 2020

Contents

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Foreword

Demetrios Marantis
Senior Vice-President, Global Government Engagement, Visa, USA

Richard Samans
Managing Director, World Economic Forum

Digital trade is more important than ever. While the COVID-19 crisis has cast a long shadow over the future of international trade in traditional goods and services, it has also demonstrated the resilience of a digitized economy and will accelerate the digital transformation of the global economy in the coming years. Digital payments are at the centre of this transformation, connecting merchants and consumers around the world and enabling new avenues for global commerce.

Thanks to new technologies and platforms, today's consumers are no longer constrained to buying from stores in their immediate community, city or even in their own country. Given this unprecedented level of interconnectedness, it is no wonder cross-border e-commerce now accounts for the fastest-growing segment in cross-border payments. This is especially important for developing markets looking to connect small businesses and microenterprises to the global economy with the fewest complications or friction as possible.

As more businesses and consumers adopt digital payments, policy-makers and regulators have an important role in ensuring payment services remain competitive, seamless and secure. Though it is easier than ever before to pay and be paid around the world, significant challenges loom on the horizon. Market barriers, diverging standards, security threats and a lack of coordination on cross-border oversight all threaten future growth in the digital economy. This report examines these issues and provides policy-makers with concrete solutions to streamline cross-border payments and promote digital trade in furtherance of their efforts to foster inclusive economic growth.

This report is part of the World Economic Forum's broader work on digital payments, which supports inclusive growth in the digital economy. The work explores ways to encourage financial inclusion, digital payment acceptance and global interoperability, covering existing and emerging technologies, including digital currencies. Through this effort, the Forum recognizes the importance of bringing the public and private sectors together to accelerate the benefits of the digital economy. This report was produced by the Platform for Shaping the Future of Trade and Global Economic Interdependence.

Executive summary

“The current COVID-19 public health crisis will only accelerate digital trade and cross-border e-commerce as physical commerce contracts and digital commerce expands.

The rapid expansion of access to digital payments has made it possible for consumers to conveniently make purchases for goods and services from merchants around the world. The current COVID-19 public health crisis will only accelerate digital trade and cross-border e-commerce as physical commerce contracts and digital commerce expands. However, significant challenges for digital trade and cross-border payments persist, providing an opportunity for policy-makers and regulators worldwide to reduce friction and improve connections between digital economies globally.

This report builds on past World Economic Forum research and leverages the Forum's extensive community of payment experts in order to move beyond the challenges and provide governments with concrete recommendations to promote inclusive growth in the digital economy. Each recommendation addresses its respective challenge as follows:

Barriers to supplying payment services

The challenge: A growing number of protectionist measures, such as domestic infrastructure requirements, forced data localization, and licensing and equity requirements for foreign service firms, prevent international payment service providers from bringing services to market. Additionally, these measures keep domestic providers from expanding abroad, which is essential for firms that want to bring their services to scale.

Recommendations

- Provide, reinforce and/or extend “**national treatment**” for digital payment service providers
- Support **commitments to protect the free flow of data** while ensuring regulatory access to data
- Create a “**reference paper**” on payment services at the World Trade Organization
- Explore creating **regional payment councils** to bring the public and private sectors together

Standards and interoperability

The challenge: The cross-border payment landscape is more competitive and complex than ever but diverging regulatory and technical standards have increased friction in making payments.

Recommendations

- Explore **digital trade agreements** to promote greater interoperability
- Establish **open banking guidelines** to spur competition and innovation
- Adopt **international standards for public infrastructure**
- Adopt **Financial Action Task Force** standards
- Work with the **international community** when developing new standards for **new technologies and regulatory regimes**

Security and trust

The challenge: Cross-border payments are disproportionately targeted by fraud and cybersecurity threats, and small businesses are particularly vulnerable. Furthermore, many policies to improve cybersecurity and trust are either ineffective or counterproductive.

Recommendations

- Establish **public-private partnerships on cybersecurity**
- Encourage **law enforcement cooperation** and **modernize mutual legal assistance treaties**
- Encourage **cyber hygiene** through government-led programmes
- Work with the private sector to establish important **consumer protections**

Innovation enabling oversight

The challenge: The adequate supervision and oversight of payment systems is integral to the safety and security of the financial system. However, the oversight for firms operating in multiple markets is often disjointed and uncoordinated, leading to inefficiencies and reduced competition.

Recommendation

- Explore bilateral, regional and multilateral **oversight coordination**

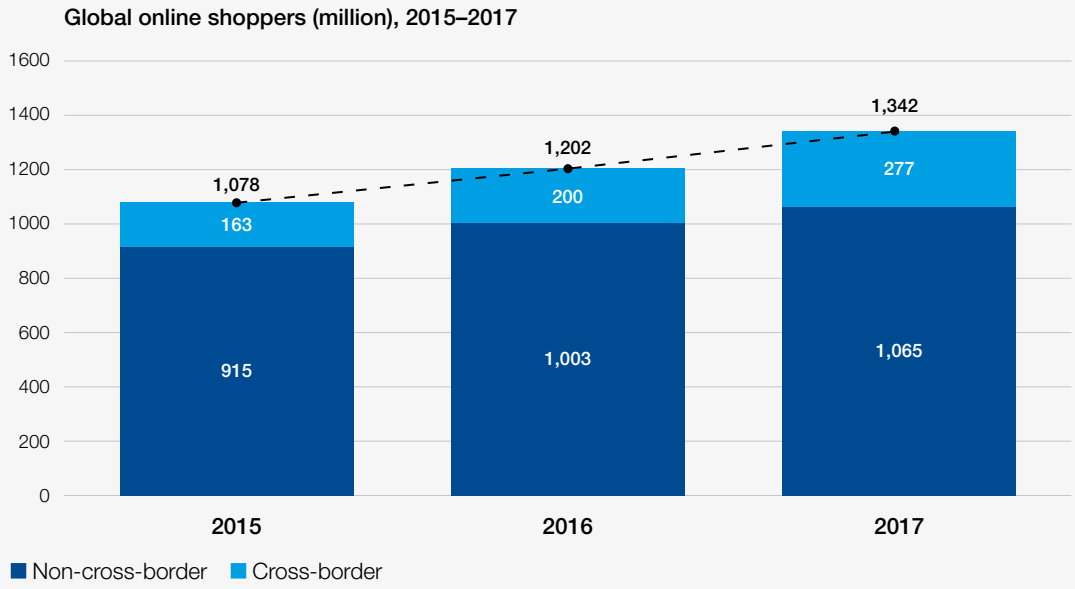
Dynamics in cross-border payments are rapidly changing, creating a network of mutually independent but highly interconnected networks. This report finds that the challenges facing cross-border payments are also highly interdependent and, therefore, holistic reforms are needed to ensure competition and reduce friction.

Introduction

Digital payments are at the centre of digital trade

Today, merchants of varying sizes can easily sell products to consumers around the world. As cross-border e-commerce expands rapidly (Figure 1), it is increasingly becoming an important component of international trade. The current COVID-19 crisis will likely accelerate this expansion, as trade in goods and physical commerce retreat and digital services advance. Digital payments are at the centre of digital trade growth and serve as the key enabling factor for digital commerce. The rapid expansion of access to digital payments has made it possible for consumers to conveniently make purchases for goods and services from merchants globally – and for merchants to sell to the world far more easily and cheaply than ever before. With a few clicks and identity verification, consumers and merchants can set up accounts to send or receive money worldwide.

FIGURE 1 **The rapid expansion of cross-border e-commerce, 2015-2017**



Source: United Nations Conference on Trade and Development (UNCATD), "Global e-commerce sales surged to $29 trillion", 29 March 2019, https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2034

In addition to enabling cross-border digital commerce, a growing body of research suggests digital payments are important to the health of the broader domestic economy. Recent studies have shown that digital payments overall increase economic efficiency, reduce crime and corruption, and support transitions away from the informal economy.[1] For instance, a 2017 Moody's Analytics study estimates that digital payment usage "contributed an additional $296 billion to consumption between 2011 and 2015, or a 0.1% cumulative increase in global GDP during the sample time period".[2]

Despite the importance of digital retail payments to cross-border commerce, significant logistical and governance challenges persist. Cross-border payments are inherently complicated and require moving funds through different entities and jurisdictions with differing rules and regulations while mitigating a wide range of risks, from fraud and cybersecurity attacks, to liquidity and foreign exchange volatility. However, while facilitating cross-border payments may never be simple, there is significant room for improving efficiency.

Today, many policy-makers are working with industry to address challenges facing cross-border payments, but additional work is needed. While significant focus has been placed on leveraging new technologies and updating infrastructure (e.g. clearing and settlement systems), the main challenge is a lack of coherent interoperability between regulatory and technical systems. The future of payments does not lie in siloed systems: making payments today requires a vast network of mutually independent networks that connect consumers, merchants, financial institutions, mobile applications, international and domestic payment networks, clearing and settlement systems, digital currencies, and other important parts of the payments ecosystem. This growing network of participants has made the payment industry more competitive than ever, but each connection between participants also presents an opportunity for friction.

Building on the World Economic Forum's past research (most notably the 2018 paper "Addressing E-Payment Challenges in Global E-Commerce"[3]) and leveraging the Forum's extensive community of payment experts, this report examines the key challenges facing cross-border retail payments and provides recommendations for policy-makers to overcome them.

In working with this community of experts, this report finds that to efficiently facilitate cross-border retail payments between businesses and consumers around the world, policy-makers need to address four key areas: market barriers, interoperability, security and oversight. This report is thus organized into these four categories, addressing challenges and recommending solutions in each section.

1 Barriers to supplying payment services

Modern trade commitments are needed to address growing barriers

Market barriers have a significant impact on firms and their ability to provide cross-border payment services because they prevent economies of scale.

Increasingly, governments are establishing significant market barriers affecting payment service providers, often in the name of security and privacy concerns. These barriers come in the form of domestic processing mandates, discriminatory licensing, foreign equity caps and forced local data-residency requirements (a concept known as "data localization"). While sometimes well intentioned, these policies often exacerbate the issues they were meant to address, with other unintended consequences.

Market barriers have a significant impact on firms and their ability to provide cross-border payment services because they prevent economies of scale, which are critical given the initial investments in processing and data storage facilities, as well as compliance with complex regulatory and operational standards. Firms reaching scale can maximize their initial investments and reduce transaction costs,[4] which is especially difficult for businesses operating in small and developing markets to achieve without being able to expand abroad. The 2017 *Global Payments Innovation Jury* report, a global survey of industry executives, found that the "inability to scale" was the biggest factor (26%) for why payment start-ups fail, followed closely by "regulation" (15%, ranked third). These restrictions impact local merchants who may not be able to use their preferred payment provider to process transactions, denying them the ability to become more competitive via exports.[5]

International networks operating in markets also play an important role in connecting domestic payments with their counterparts in other countries, and these connections can be hindered by regulatory discrimination against international networks. Furthermore, ensuring local competition also meets other policy objectives, especially financial inclusion, as increased competition lowers costs and thereby augments access to financial services.

Given these barriers, existing trade commitments and cooperative frameworks governing payment services are insufficient to support modern trade needs. To meet these needs, modern trade commitments on digital payments are necessary. This section analyses three key types of barriers to payment services before providing best practices and recommendations for policy-makers on how to improve the role of payment services in global trade.

BOX 1 **Current World Trade Organization commitments on payments**

As outlined in the World Economic Forum's paper "Addressing E-Payment Challenges in Global E-Commerce", World Trade Organization (WTO) rules on the cross-border supply of digital payments (or "electronic payment services") are found in the General Agreement on Trade in Services (GATS) and its Annex on financial services. The Annex and subsequent WTO panels define electronic payment services as "all payment and money transmission services" and "all services essential to payment and money transmission, all means of payment and money transmission (i.e. paper-based, card-based and others), and all associated business models".[6] General commitments (for all WTO members) require members to treat all foreign suppliers of payment services equally. Specific commitments (for WTO members who have agreed to additional market access) include market access and/or non-discrimination of foreign supplier (national treatment) for cross-border supply (Mode 1) and establishing commercial presence (Mode 3).

WTO member commitments under GATS on payment services are limited and patchy.[7] For example, only 53 WTO members have fully or partially liberalized the cross-border supply of "payment and money transmission services".[8] Currently, only 18% of WTO members have full cross-border supply commitments (Mode 1) for all payment and money transmission services, and only 14% have full commercial presence commitments (Mode 3).[9]

1.1 Domestic infrastructure/processing requirements

Many countries are enacting indirect barriers to foreign payment providers via rules about how and where payment transactions can (or cannot) be processed. Some countries are enacting laws that require all domestic transactions to be processed by a single local "switch", which is a processer that facilitates communication between various providers involved in processing a transaction. Often these requirements are motivated by the belief that these barriers are necessary to support the domestic financial services sector, to provide lower cost options to expand access, or to increase security through direct regulatory oversight of the payment system.

Similarly, some countries require that all domestic transactions be processed onshore (i.e. forced local processing). This, like forcing firms to use local switches, is another way to create an unlevel playing field, as these regulations force international payment networks to duplicate their global capabilities in-market by building a local data centre or simply exclude them from processing domestic transactions.

Examples of countries enacting local processing requirements are far-reaching. In 2011, Nigeria's Central Bank introduced a measure that requires

all domestic point-of-sale, ATM and digital transactions to be processed locally.[10] In 2014 and 2016, the Russian Federation enacted new payment system laws that force international payment providers that want to operate in the country to transfer their processing capabilities with respect to their domestic operations to a local state-owned operator.[11] Indonesia has enacted new rules that effectively prohibit foreign firms from playing a role in domestic payments, as part of its initiative for a domestic payment gateway.[12] The new rules require all domestic electronic (i.e. non-cash) transactions to be stored locally and processed through this domestic gateway provider. Finally, Viet Nam has proposed a mandate to require all payment processing through a single, state-owned firm, but has delayed implementation over trade concerns.[13]

1.2 Forced data localization

“ Data localization has negative effects for both foreign and domestic payment service providers.

Local data storage requirements – known as data localization – act as a barrier to market entry and operations for payment service providers. These requirements hinder cross-border payment services because data is essential in every step of transaction processing.[14] The supply of payment services often requires the cross-border flow of data, not only in settling cross-border transactions, but also in purely domestic transactions, when both the merchant and the consumer are located in the same market but the processing of the transaction (or parts of it) are carried out elsewhere.[15]

Countries enact data localization in response to technological innovation for a variety of well-intentioned but misguided reasons, such as to address privacy and cybersecurity concerns, to allow their government’s access to payment data, and to encourage domestic industries and economic growth. However, a growing body of research suggests that data localization fails to achieve many of these goals and adds significant costs to the local economy, reduces data security and does not improve consumer privacy.[16] For instance, a now widely cited McKinsey analysis reports that open data flows more broadly are actually critical to future economic growth and likely increased world GDP by 10.1% over the past decade.[17]

Data localization has negative effects for both foreign and domestic payment service providers. It discriminates against foreign firms as it makes their services more costly or complicated in comparison to local firms, while local firms are more likely to use local data storage services. However, many local firms (especially start-ups) increasingly rely on cloud computing services to manage data and process transactions, which would be prohibited under many data localization measures.[18] In this way, many of the costs of data localization are not passed along to foreign companies but to local start-ups, financial institutions and, ultimately, consumers. Furthermore, data localization requirements impede the free flow of data, which affects the use of integrated, secure and efficient payment systems worldwide, with consequences for innovation, fraud and security.[19]

Some recent examples of data localization illustrate how countries are restricting the movement and storage of data. In 2013, Turkey enacted a law requiring firms to maintain documents, records, data storage and processing facilities in Turkey

for 10 years.[20] Turkey refused to grant a licence to foreign payment firms that failed to store data locally, subsequently causing some to withdraw their services from Turkey.[21] In 2018, the Reserve Bank of India issued rules that required payment service firms to store all transaction data locally.[22] For cross-border transactions, a copy of the domestic component may also be stored abroad but, if data is processed outside of India, the data will only be stored in India afterwards.[23] As per the Russian laws mentioned above, this requires local data storage as well as local processing.[24] The Central Bank of Brazil also proposed a cybersecurity policy that would have required data to be stored locally, including financial data, but later retracted this due to concerns over its potential economic impact.[25]

1.3 Licensing and equity requirements for foreign firms

Countries are also using restrictive licensing and equity requirements to limit the cross-border supply of payments in their markets.[26] Policy-makers do this for many reasons, such as to use forced joint ventures to help local firms become more competitive and as an outdated way to ensure oversight of local firms. However, these requirements often have unintended consequences, including reduced foreign direct investment and access to products and services from payment companies, both of which have implications for cross-border payment efficiency.

Equity regulations requiring that a local entity maintain a majority share are particularly obstructive to cross-border payment services. These requirements give international payment service providers little incentive to invest locally and bring services to markets, as they would have little or no ability to maintain governance of local affiliates and set scheme rules. *Scheme rules* outline rules and technical standards for how transactions are made and processed and apply to all participants in the network. It is important to note that while scheme rules for international networks may be set internationally, domestic governments still have regulatory authority over how they are implemented locally.

A few recent examples demonstrate the extent of equity requirements and their level of severity. In 2019, Ghana enacted the Payment Systems and Services Act, which among other things sets out the requirements to obtain a payment systems operator licence.[27] In particular, it calls for firms to establish a local entity, at least 30% local ownership, and a board of directors that includes at least three Ghanaians (one of which must be the CEO). Similarly, in Indonesia, critical players in the payment network must be appointed or approved by the central bank and must be 80% domestically owned.[28]

1.4 Recommendations: Best practices, initiatives and next steps

Current market barriers need to be reduced to improve cross-border payment efficiency and decrease costs and access constraints for local markets. New trade rules for digital payments could make this happen, and safeguarding the cross-border supply of payments in order to help innovative FinTech companies to scale globally will be critical for future trade discussions.

Unfortunately, there has been a distinct lack of progress at the multilateral level on payment services since the GATS came into force in 1995 (see Box 1). Thankfully, some countries and regions are pursuing new policies and commitments to remove market barriers for payment providers and reduce cross-border payment friction. This section focuses on core principles and several initiatives that policy-makers may wish to consider. Together, these proposals reinforce the basic foundations and architecture of the WTO, while adding new rules and regulatory best practices for an updated, open and competitive payment services framework.[29] Beyond new and meaningful market access commitments, the goal of these regulatory cooperative initiatives is to build interoperable regulatory systems that support digital trade and build trust between respective systems on cross-border payments and e-commerce.

Provide, reinforce and/or extend "national treatment" for digital payment service providers

At the most fundamental level, countries should provide (or reinforce) the basic WTO principle that they treat domestic and foreign payment services and service suppliers the same – known as national treatment – and ensure that this applies to the various modes of supply in their payment services commitments in trade agreements.[30] This is in addition to the even more foundational step that countries should take in providing meaningful payment service market access. As highlighted above, many countries have not made these basic commitments under GATS.

Countries should provide the basic WTO principle that they treat domestic and foreign payment services and service suppliers the same.

As more countries make these commitments, it will be more difficult for local markets to establish discriminatory measures that undermine the competitiveness of the payment sector. Furthermore, the WTO dispute settlement system has demonstrated that current agreements provide protection against discriminatory measures on the cross-border supply of financial services, such as the GATS Annex on Financial Services,[31] and therefore should be enforced. First, a WTO panel establishes that the supplier's presence or operation in the destination market should not be required for cross-border supply, where members have made a commitment to allow the cross-border supply of a service.[32] This is relevant to data localization provisions – given it makes supply contingent on them setting up local computing facilities – but it has never been tested in a trade dispute. Second, a WTO panel establishes that GATS is technologically neutral in terms of how a service is supplied, in that commitments do not differentiate between mail, telephone or the internet.[33] Third, a WTO panel reinforces the broad definition of payment services outlined in the GATS Annex on Financial Services, in that it includes "all payment and money transmission services, including credit, charge and debit cards, travellers cheques and bankers drafts".[34]

Regional and bilateral trade agreements provide another opportunity for countries to further reduce market barriers and cross-border frictions for payment services. For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) reinforces and goes beyond WTO provisions on financial services but is still limited in the scope of its commitments. The CPTPP includes an annex with specific commitments on payment services, which could in theory limit the imposition of regulatory requirements to locate data storage and processing facilities in each country.[35] However, the CPTPP does not guarantee non-discriminatory treatment as countries can provide preferential treatment to local e-payment service providers as long as foreign networks also have a right to supply. Additionally, the CPTPP definition of electronic payment services for card transactions is fairly restrictive in that it focuses on credit card networks and business-to-business transactions. Various side letters between CPTPP members also authorize existing measures that discriminate against foreign payment providers, such as via local presence requirements.

Support commitments to protect the free flow of data while ensuring regulatory access to data

In theory, GATS commitments should prohibit data localization requirements where a country has made market access commitments, as the cross-border transmission of data constitutes the service being supplied (and thus blocked via data localization).[36] Forced data processing and storage also discriminate between local and foreign providers, thus breaching national treatment commitments.[37] They also breach provisions in the GATS Annex on Telecommunications, which ensure that foreign-service suppliers are allowed to use basic telecommunications for the movement of digitized information.[38] Despite this, data localization is proliferating. To upend this trend and reduce cross-border payment friction, specific commitments prohibiting data localization requirements are needed in future WTO and regional trade agreements.

Several bilateral and regional trade agreements have already done this, including provisions to protect the free flow of data and prohibit data localization. Unfortunately, the broad data flow provisions in the CPTPP's e-commerce chapter that prohibit barriers to data flows and forced localization do not apply to financial services, including payments.[39] However, the financial services chapter does include the commitment to allow financial institutions of the other parties to "transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business".[40] The applicability of this section is uncertain, as it leaves each party to determine who is a "financial institution".

The United States–Mexico–Canada (USMCA) trade agreement goes further than the CPTPP in providing explicit, detailed protections for the free flow of data and prohibitions on data localization in the financial services chapter,[41] and serves as a model for agreements on digital trade. The USMCA's financial services chapter also applies explicit national treatment to payments and market access to firms from other parties.[42] These include payments via credit cards, charge cards, debit cards, travellers cheques and bankers drafts, but not securities transactions.

The USMCA also provides a clear framework to allow the free flow of data, while ensuring parties have regulatory access to data.[43] This is an important development as many policy-makers try to justify data localization on the belief that it is necessary to ensure a government's access to the data. In the era of cloud computing, however, data can be provided with a few clicks of a mouse button, while still allowing firms to move financial data freely in order to provide secure, innovative, globally deliverable services. USMCA parties agreed to "recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access".[44] The USMCA's focus on regulatory access is made clear with a provision that prohibits parties from requiring financial firms to use local computing facilities as a condition of doing business "so long as the Party's financial regulatory authorities … have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory".[45]

TABLE 1 **Commitments on digital payment services by trade agreement**

Commitment	WTO	CPTPP	USMCA
National treatment	Optional	Optional	Yes
Market access	Optional	Yes	Yes
Explicit data localization prohibition	None	Yes, but financial services are exempted	Yes

Create a "reference paper" on payment services at the World Trade Organization

Likeminded parties that recognize and support a competitive payment sector could compile these rules into a digital payments "reference paper", akin to adding payment services and updated and additional commitments to the WTO "Understanding on commitments in financial services". This "Understanding" was not part of the GATS but was appended to the Uruguay Round as an alternative (and optional) way for the countries (31 WTO members) that wanted to make specific additional commitments in financial services.

Like the WTO's "Telecommunications Services Reference Paper", a reference paper for payment services could include common principles and best practices to support payments competition and a framework that reinforces, and is adaptable to ever changing, financial and payments innovation.[46] Such a paper should also establish a detailed set of obligations related to financial data, operations, processing requirements, the role of state-owned enterprises and regulations for renewed commitments by relevant parties. For example, it could build on the CPTPP commitment of parties to allow financial institutions of other parties to supply new services (in line with the principle of national treatment).[47]

Such an initiative would be grounded in regulatory cooperation and interoperability (as opposed to harmonization). It could include provisions that reinforce national treatment for payments, an analysis of market access commitments for payment services and associated information and communications technology services, and cooperation on regulation, such as risk-based know-your-customer rules and common licensing produces.

Explore creating regional payment councils to bring the public and private sectors together

The barriers outlined above start as well intentioned policies but have many unintended consequences. To address some of these barriers' initial policy goals, such as ensuring local economic development and data privacy and security, some countries and regions are establishing *payment councils* to create a public-private dialogue on payment policy issues. For example, the Monetary Authority of Singapore (MAS) set up the Singapore Payments Council comprising 20 representatives from payment service providers, financial institutions, trade associations and merchants. The council's goal is to encourage collaboration within the payment industry, make recommendations on policies and develop strategies to ensure efficiency, competition and interoperability within the payment industry.[48] A similar initiative exists in Brazil but is focused on a specific goal. The Brazilian Central Bank established the Instant Payments Forum, a permanent advisory committee with over 200 members from the Central Bank, financial institutions and other institutions, to collaborate and discuss matters regarding instant payments.[49]

> To address some of these barriers' initial policy goals, such as ensuring local economic development and data privacy and security, some countries and regions are establishing payment councils to create a public-private dialogue on payment policy issues.

Moving beyond domestic payment councils, recent public- and private-sector collaboration in ASEAN could be a good model for regional cooperation on payments. ASEAN is a dynamic and tech-savvy region, but its members have differential and sometimes conflicting rules and regulations for payments. Like most other regions, there is no cross-border payment system in ASEAN.[50] However, ASEAN has made the integration of the region's digital market a top economic priority and has recognized the importance of improving cross-border payments. To assist the ASEAN Secretariat in these efforts, the World Economic Forum launched a public-private initiative called the ASEAN e-Payments Coalition, which is working with the ASEAN Working Committee on Payment and Settlement Systems (made up of central bank representatives) to develop a regional payment framework that improves user payment experiences, promotes regional integration, increases trust and security, and improves the livelihoods of the underbanked.[51] This model could also be adopted internationally, especially for intergovernmental organizations focused on financial services, such as the Bank for International Settlements (BIS).

This type of public-private collaboration is critical to any policy decision related to cross-border payments and is not limited to issues regarding market access. Payment councils are also a good place to formulate policies on issues concerning standards, interoperability, security and regulatory oversight, which are discussed in further detail in the following section.

2

Standards and interoperability

Internationally accepted standards are critical to improve connections

Advances in technology and regulatory reforms have led to a renaissance in digital payment innovation. While the appearance of new payment providers and technologies has led to new innovations and increased competition, it has also led to an increasingly complex set of systems with significant variation in standards by region, making cross-border payments increasingly difficult. While many of these new systems provide value for consumers, the interoperability between systems is increasingly complicated. Broadly defined, interoperability enables all participants of the payment system (e.g. consumers, merchants and governments) to easily send funds between different payment networks and instruments.[52]

Paradoxically, this is further complicated by uneven attention from policy-makers, who may promote the adoption of international standards while pursuing domestic technical standards, which creates other frictions with making international connections.

These two factors – new technologies and regulatory fragmentation – have created significant interoperability challenges and increased difficulty in making and receiving cross-border retail payments. Countries can take steps, however, to reduce this friction and move towards greater harmonization and interoperability. International standards are critical to promoting interoperability and ubiquity in the global payment system, but the adoption of certain international standards is uneven and the need for new international standards is growing as new technologies and regulatory proliferate. Yet standards adoption and creation in specific areas could encourage greater interoperability.

2.1 Uneven adoption of international standards creates cross-border friction

Connections between payment systems are facilitated through a complex set of relationships and messaging systems, many of which are governed by international standards. For instance, standards governing messaging play an important role in facilitating cross-border payments. Many payment card networks connect consumer banks (issuers) with merchant banks (acquirers) using a common messaging standard (International Organization for Standardization (ISO) 8583). Similarly, cross-border payments sent between banking customers also use international standards and standardized messages between banks with instructions for payment transfers (e.g. using a standard such as ISO 20022).[53]

“Interoperability can be further stymied by participants wary of sharing too much data across other networks, viewing consumer data as proprietary and essential for maintaining a competitive advantage.

Despite the availability of mechanisms for making connections between payment networks, some challenges still exist. Many financial institutions are still operating on older messaging systems that do not easily connect with newer systems and cannot pass along sufficient information to facilitate cross-border transactions – for instance, information needed to comply with anti-money laundering (AML) or other regulatory requirements. Furthermore, regulators are playing a more active role in setting a range of payment standards, from encryption to how transactions are authenticated and consumer information is secured. (For more on authentication standards see the following section on security and trust.) Many of these domestic standards conflict with international standards and add additional friction to cross-border payments. Some of this friction could be intentional, as requirements to use domestic proprietary standards have long been used to tilt the competitive playing field in favour of domestic payment firms.

Interoperability can be further stymied by participants wary of sharing too much data across other networks, viewing consumer data as proprietary and essential for maintaining a competitive advantage. To increase data sharing and encourage interconnectivity and competition among payment providers as well as other financial service providers, many countries are embracing *open banking*. Open banking refers to consumers sharing their banking data with third-party applications and firms in order to access new and innovative financial services.[54] According to the *Open Banking Report 2019*, at least 50 countries have some kind of open banking initiative, involving some 10,000 financial institutions.[55] Financial regulators have taken a variety of approaches to support open banking, some with explicit requirements for banks to share data with licensed third parties for additional services (including payment initiation) and others with guidelines meant to champion data sharing and common API standards.[56]

While open banking initiatives are likely to encourage more interoperability in the long run, diverging domestic standards for open banking are likely to present significant challenges to cross-border interoperability in the immediate future. Further, despite open banking’s growth in popularity, no coordinated international effort is in place to set standards.[57]

In addition, standards and practices on AML, combating the financing of terrorism (CFT) and know-your-customer (KYC) requirements across countries need to be coordinated for payment systems to be connected. AML/CFT systems and the implementation of customer due diligence on cross-border payments currently vary across countries, although countries are attempting to meet a set of global standards. As reflected in the Financial Action Task Force (FATF) consolidated

ratings of 30 April 2020 – which show the results of countries' compliance with the FATF's 40 recommendations for fighting money laundering and terrorist financing[58] – countries have different levels of AML/CFT compliance and effectiveness related to cross-border payments.[59]

The current practice in most countries of requiring in-person identity verification based on multiple paper documents by a financial service provider and repeating the process each time the customer opens an account can impose significant costs to both the service provider and the customer. As part of a Committee on Payments and Market Infrastructures (CPMI) survey, respondents noted legal, regulatory and compliance considerations as the most significant cost and challenge to their business, especially for cross-border payments; in particular, payment service providers cite AML, KYC, risk mitigation and consumer protection requirements.[60] The requirements can be a major hurdle to efficient payment services and financial inclusion in cases where individuals and small businesses do not have the ID documentation needed to open an account. All of this combined with conflicting domestic standards on KYC (often with little guidance or with prohibitions on the digitization of these requirements) and a lack of common rules governing digital identity can add additional friction in cross-border payments.

2.2 Recommendations: Best practices, initiatives and next steps

To reduce friction in cross-border retail payments, governments should encourage the adoption of internationally accepted standards whenever possible. By having a common set of standards, participants in the payments ecosystem can send and receive payments across borders with less need for domestic customization and human intervention. The adoption of international standards will also increase competition in local markets by reducing barriers to entry for other third-party payment providers, such as FinTechs. In addition, it will reduce barriers for domestic firms seeking to expand abroad, which is especially important for small and developing countries that want to bring their FinTech start-ups to scale.

Explore digital trade agreements to promote greater interoperability

“Open banking provides a good alternative for governments seeking data localization policies to encourage local competition.

As with other service industries, an effective way to encourage interoperability and international harmonization is through trade agreements. But as discussed in the previous section, current trade agreements governing digital payments are insufficient at meeting the needs of the new technology platforms and service providers. New commitments to adopt internationally accepted standards would provide incentives for domestic industries to promote them by ensuring reciprocity among trading partners.

A few recent egional trade agreements serve as good examples. The recently finalized Digital Economy Partnership Agreement (DEPA) among CPTPP countries Chile, New Zealand and Singapore is novel in both its handling of the digital financial services and its focus on digital payments. While payments and financial services more broadly are excluded from many of the DEPA's commitments (which raises other issues, as discussed), the agreement does have a dedicated chapter on digital payments (2.7) with a focus on international standards. Signing parties of the DEPA commit to “agree to support the development of efficient, safe and secure cross-border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability and the interlinking of payment infrastructures, and encouraging useful innovation and competition in the payments ecosystem”.[61]

A further innovation of the DEPA is the first of its kind promotion of open banking in a trade agreement. Parties agree to stimulate the use of open APIs and advise third-party players to “facilitate greater interoperability and innovation in the electronic payments ecosystem”.[62] By committing to adopt internationally accepted standards and boost data sharing between payment providers, the DEPA seeks to increase interoperability and promote a more seamlessly integrated network of networks for digital payments. This additional commitment rounds out DEPA's holistic approach to reducing cross-border payment friction, which takes into account the full value chain of interconnected payment networks.

While the agreement is currently only between three countries, DEPA's innovations in actively promoting open banking, interlinking payment infrastructure and supporting common payment standards could serve as a template for encouraging interoperability for broader WTO discussions on e-commerce and digital trade.

Establish open banking guidelines to spur competition and innovation

Government guidelines on standards can be another effective way to endorse the adoption of internationally accepted payment standards.

Guidelines on open banking, in particular, can both foster interoperability and increase competition. Governments have taken different approaches to open banking, with some preferring strict mandates for technical standards and data sharing, and others favouring voluntary guidelines meant to urge greater cooperation within the payment sector. Given the payment industry's technical expertise in payment standards, often setting voluntary guidelines is enough to stimulate common standards adoption and increase interoperability.

Singapore's recent experience with open banking provides a good example of the public and private sectors working closely together to develop a common set of guidelines to increase interoperability and competition. In 2016, the MAS worked with the Association of Banks in Singapore to develop guidelines on API and security standards.[63] The MAS also developed a comprehensive list of open APIs to encourage greater connectivity between FinTechs and financial institutions.[64] The MAS itself opened 12 public APIs for data handled by the monetary authority to demonstrate its commitment to the initiative. Shortly thereafter, financial institutions (such as Standard Chartered and DBS) and payment companies (such as NETS, a Singapore-based payment company) launched developer platforms and e-wallets based on MAS guidelines.

Open banking also provides a good alternative for governments seeking data localization policies to encourage local competition. As noted, policy-makers often require data localization to foster growth among domestic firms by protecting them from foreign competition, which comes at a great cost. Open banking also promotes growth among domestic firms but does so by lowering barriers to entry for new service providers, which in turn prompts greater competition in the domestic payment services market. Furthermore, open banking advances domestic growth without raising the costs of computing services or cutting them off from international networks and cloud computing services. This is especially important for developing countries and other markets with a nascent FinTech sector, as localization can hurt start-ups dependent on international network connections and cloud computing services.[65]

Open banking can also address financial inclusion concerns often raised by regulators pursuing localization policies, by lowering costs and entry barriers for new financial firms and by providing new sources of data to provide a more complete credit profile for the underbanked. While open banking to date has primarily focused on consumers with formal bank accounts being able to share data between financial service providers, open data principles could be expanded to other payment services, including those using a third-party agent (rather than a bank account) to access funds. This would spread the benefits of open banking to underserved populations, especially in markets

where access to accounts at financial institutions remains limited. Beyond financial data, open data for utility and telecom payments could further extend the benefits of open banking regimes to underbanked populations, as these accounts are more widely used than accounts at financial institutions in some markets.[66]

Adopt international standards for public infrastructure

Governments can also lead by example and encourage interoperability by adopting internationally accepted standards in public projects to modernize infrastructure, such as real-time payment systems. Real-time payment systems, also known as instant or faster payment systems, refer to interbank payment systems that enable near real-time clearing and availability of funds, as well as continuous service availability.[67] At least 54 countries now have real-time payment platforms and many more are planned.[68] While many of these new systems are primarily designed to facilitate bank-to-bank payments, the implications for retail payment systems are significant as well, as many enable third-party connections (e.g. for FinTechs and payment networks) and retail payment initiation.

Forward-looking central banks managing the development of real-time payment systems are using this as an opportunity to update messaging standards and support broader financial system modernization. Specifically, central banks are adopting ISO 20022[69] as the messaging standard for new systems, an internationally accepted standard that enables participants in the payments ecosystem to send richer information on transactions than in the past. Further, central banks should collaborate closely with industry groups already working on international standards harmonization, such as the Payments Market Practice Group, which is leading efforts to define usage guidelines for consistent use of ISO 20022 in cross-border payments.

“ Adopting the same standard as other payment systems reduces the costs associated with integrating with the other systems.

The adoption of ISO 20022 could reduce cross-border payment friction in two important ways. First, central banks sharing a common messaging standard will be able to make more transactions and pass along richer information important for clearing transactions (e.g. KYC information, AML/CFT reporting, etc.). Second, by adopting an international standard for important financial infrastructure, payment providers wishing to connect with this infrastructure have an economic incentive to modernize their messaging systems and adopt new standards. This in turn could have multiplier effects throughout the broader ecosystem, in which players use common standards to send messages to each other and within their own payment networks, either through a real-time payment system or through other open, interoperable networks. Finally, adopting the same standard as other payment systems reduces the costs associated with integrating with the other systems.

Modernization will take time, however, and it may not be feasible or advisable for all markets. Many financial institutions facilitate payments through older, though still internationally accepted, standards (e.g. financial transaction card originated messages standard ISO 8583[70]). These standards still enable interoperability but are not always able to pass along the richer information needed to facilitate cross-border payments.

Additionally, modernization will also be costly for participants, especially for larger financial institutions, so central banks should expect multiple international standards to run in parallel in the near term.[71] Costs may be a significant impediment for developing nations as well, so new financial infrastructure and broader modernization projects should be evaluated in parallel with other priorities given initial implementation costs.

Adopt Financial Action Task Force standards

The adoption of FATF standards is important to the integrity of the financial system. A consistent and international approach is necessary to achieve the FATF objectives of fighting financial crime and to level the playing field and avoid the risk of exploitation of weak links in the financial system. Any country that fails to adopt the international standard leaves the entire financial system vulnerable to criminal activity abuse, particularly given the inevitable cross-border nature of money laundering.

Enabling bilateral or multilateral cross-border solutions would require all countries to have mutual confidence that each domestic network’s AML/CFT system is adequate. In this regard, countries should ensure that they bring their AML/CFT system, particularly the aspects related to customer due diligence, in line with the FATF standards. Additionally, consistent reporting across jurisdictions would ease the compliance burden.

Countries are encouraged to align their AML/CFT legal framework with the FATF standards and focus on basing their payment system principles on risks and outcomes. To facilitate financial inclusion without undermining financial integrity, customer identification/verification regulations could require regulated providers to have a reasonable basis for knowing who their customers are, but without rigidly prescribing how they are to achieve this objective. Under such a system, individuals without adequate identity documents can undergo tiered client due diligence and progressively expand their level of access to financial services, beginning from a restricted, low-risk type of account. Over time, as the regulated provider treats the data generated by the customer’s activities as identity evidence, it can expand the functionality and threshold of the account offered to the customer.

The recently issued FATF Guidance on Digital ID offers a risk-based approach to the use of digital forms of identification for customer due diligence (CDD) purposes. The Guidance recommends that national governments encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion, and consider providing guidance on how to use digital ID systems with different assurance levels for identity proofing/enrolment and authentication for tiered CDD. The guidance sends a clear message that authorities need to take a proactive role in either assessing themselves the relevant assurance levels of a digital ID (or nominating another body to assess them) or providing guidance on how this should be done. Regulated entities such as financial institutions should consider whether digital ID systems with lower assurance levels are sufficient for simplified due diligence in cases of low money laundering/terrorism financing risk.

One way countries are seeking to encourage financial inclusion while ensuring financial system integrity is through e-KYC initiatives. e-KYC digitizes the manual KYC process, potentially reducing the costs of engaging new customers while complying with AML/CFT requirements. Centralized, digital identity databases would support e-KYC systems by linking local identity proxies with digital identity databases. These systems can significantly reduce transaction costs for service providers and customers and can also enable greater access to bank accounts. An example is Pakistan's National Database and Registration Authority, which makes it possible for consumers to more easily open digital wallets using biometric data, allowing branchless banking. In 2015 alone, digital wallet accounts tripled from 5 million to 15 million.[72] Similar projects have been launched in Africa, such as Nigeria's Bank Verification Number project, which enables consumers to use mobile phones to verify their identity by matching the information with a network of financial institutions connected to the Central Bank of Nigeria's database of biometric information.[73]

"It is important in the long run to work with international standards organizations to achieve international harmonization.

Work with the international community when developing new standards for new technologies and regulatory regimes

Many nations recognize the importance of international standardization and face challenges when governing payment issues where no international standards exist. While efforts to fill governance gaps with novel domestic standards are laudable, they may introduce new frictions in cross-border digital commerce as countries adopt other, non-conforming standards. Furthermore, the pace of payment technology is rapidly progressing, and most governments would do better to take a subdued, technology neutral approach to accommodate new innovations.

Fortunately, certain mechanisms allow countries to coordinate the development of payment standards and encourage cross-border interoperability without waiting for international standards to be developed. First, some countries are developing domestic standards and guidelines while entering into bilateral agreements that recognize other domestic standards in order to reduce friction in cross-border commerce. For example, the MAS recently signed several bilateral cooperation agreements on FinTech covering standards-related issues. A recent agreement between the MAS and the Central Bank of Kenya states both parties agree to co-develop "digital infrastructure services […] based on a set of common standards".[74]

Second, some governments are launching new domestic standards to meet local needs in coordination with international standards experts so that domestic standards might scale internationally in the future. For example, in 2016 the Reserve Bank of India worked with various payment service providers on an initiative to increase consumers' and merchants' access to payments as well as interoperability between domestic and international payment systems.[75] Through this effort, the Reserve Bank of India set guidelines for payment companies to use a common QR code (*Bharat QR*), which ultimately became the basis for the internationally accepted EMVCo standard. This interoperable standard enabled merchants to accept both payments from domestic payment service providers as well as international providers using a single acceptance code. Other governments have followed India's example, and even the entire ASEAN region is considering adopting the same standard to further encourage regional interoperability.[76]

Third, the number of regional forums for coordinating standards development and mutual recognition is growing. Again, ASEAN provides a good example of regional cooperation on payment issues. The *ASEAN Economic Community Blueprint 2025* outlines a number of areas for economic cooperation among member states, including the goal of "financial integration".[77] ASEAN has deemed this issue important enough to establish the Working Committee on Payment and Settlement Systems (WC-PSS) to develop a framework for financial integration, which will include principles on the "standardization of innovative retail payment instruments".[78] Local industry players should play an important role in discussions on regional standards, particularly through the already established ASEAN e-Payments Coalition mentioned earlier.

Finally, while bilateral and regional cooperation efforts are laudable, it is important in the long run to work with international standards organizations to achieve international harmonization. Intergovernmental organizations (e.g. the Bank for International Settlements) as well as industry organizations (e.g. EMVCo) continue to work to develop standards and guidelines for governing emerging technologies, which is critical to the future of cross-border digital commerce.[79]

3

Security and trust

The mitigation of fraud and cyber-threats is critical to digital commerce

Technology-enabled innovation in financial services presents many opportunities for cross-border payments and digital trade, but also raises concerns about cybersecurity. A 2017 PricewaterhouseCoopers survey found that 85% of consumers believe that cybersecurity risks are among the greatest facing society.[80] Financial firms are particularly focused on cybersecurity as they are 300 times more likely to be subject to a cyberattack than non-financial firms,[81] with the economic impact of cybercrime estimated at well over $600 billion per year.[82] Thus, an understanding of the challenges, best practices and needs in the cybersecurity ecosystem is paramount to the future growth of cross-border payments and digital trade.

A multitude of actors are typically involved in a cross-border payment, particularly when it is linked to digital trade. Each link in the chain could pose a cybersecurity risk. Moreover, the rise of digital trade has meant that individual consumers and small businesses are making more cross-border payments than ever before. Digital small and medium-sized enterprises (SMEs) are a prime target for cyberattacks. In a 2017 global survey of e-commerce SMEs, cybersecurity/data privacy and digital reputation were listed as the top global risks.[83] As more SMEs and consumers embrace cross-border e-commerce, understanding the unique challenges they face is essential.

3.1 Rising fraud and cyber-risks

5bn
The number of mobile users worldwide

There are over 5 billion mobile users globally.[84] Over 60% of these are smartphone connections. The set of risks for both feature phone and smartphone users continues to grow and includes the following:

- **Feature phones** – These phones can operate with poorly protected hardware and software and often lack an operating system that uses the latest security solutions.
- **Social engineering** – Social engineering involves deceiving users into divulging information or taking action that could compromise security. The prevalence of personal information readily available online can enable a scammer to use small amounts of information to gain trust from a user and secure deeper and more personal information.
- **SIM swaps** – On both feature phones and smartphones, a hacker can use social engineering to get key personal information from users and then leverage that information to convince telecom operators to open access to phone calls and SMSs intended for the users. Transactions relying on SMS as the primary mechanism are particularly vulnerable.
- **Phishing** – Over 90% of all cyberattacks globally start with a phishing email. Phishing has been recognized as the most likely first step in attacks by cyberterrorists.[85] Protecting one account from phishing could therefore protect an entire organization, industry, or even nation.
- **Ransomware** – Malware enables a fraudster to install malicious software on a user's system to manipulate, remove or temporarily block data. Increasingly, fraudsters demand that users pay money to restore their systems. The prevalence of public Wi-Fi networks, free phone charging stations and other public network touchpoints makes the installation of malware ever easier.
- **Enterprise data breaches** – The best cybersecurity practices are typically in place at large institutions with large data caches, but those systems are also significant targets for cyberattacks. The average data breach costs an enterprise nearly $1.5 million.[86]
- **Lack of cybersecurity literacy** – Hackers typically target unsophisticated users through social engineering and phishing attacks. A Stanford University study on fraud found that online purchase scams have the highest victimization rates and are the most likely to result in fraud.[87] Small businesses are a major target due to their lack of sophistication regarding cybersecurity. A study found that 60% of small business data breaches are the result of negligent employees or contractors.[88]
- **Distributed denial of service (DDoS) attacks** – Hackers can take control of several computers using social engineering techniques and then direct those computers to communicate with a single server or computer at the same time, effectively overloading those systems and incapacitating them. Taking down a network can almost be as effective as installing malware and can have similar consequences.

3.2 Regulations on cybersecurity

Governments worldwide have responded to the multitude of challenges associated with cybersecurity by creating new regulations. These regulations exist both as comprehensive industry cross-cutting laws (e.g. Singapore's Cybersecurity Act of 2018) and rules focusing on particular industry segments (e.g. the Monetary Authority of Singapore's Notice 655 on Cyber Hygiene). Some governments have chosen to mandate data localization as part of their requirements on cybersecurity.

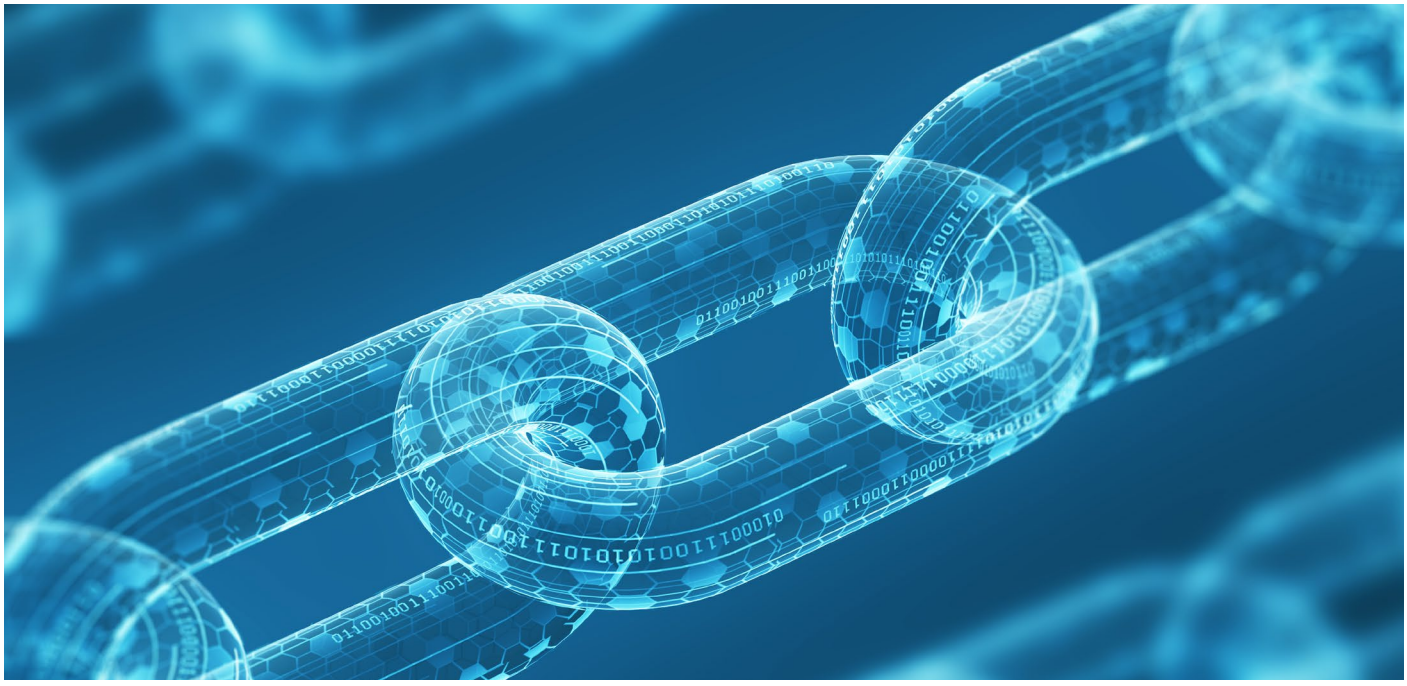
As noted earlier, data localization mandates have many negative economic consequences, but they also reduce cybersecurity. Data localization increases the number of points of potential vulnerability in a data system and takes resources away from providing maximum protection to the existing network. Data management and security are paramount to digital businesses, and the selection of where to build data centres is heavily focused on security. Security networks are only as strong as their weakest link. Proliferating data centres will reduce businesses' ability to maintain security, and newly formed data centres in particular will be subject to security threats. Spreading to multiple regions without a business case – only due to a local mandate – could lead to relaxed security practices in order to mitigate costs.

3.3 Diverging authentication/security standards

Both the public and private sectors engage in efforts to mandate standards as a tool to effectively counter cybersecurity risks. The technical nature of cybersecurity lends itself well to the creation of standards. However, the divergence in standards has created gaps in the provision of adequate security for systems and unnecessary frictions in cross-border payments.

The private sector has established several standard setting organizations related to cybersecurity. The Payment Card Industry Data Security Standard is an example of a private-sector-led standard that has become a model for retail payments. Domain-based Message Authentication, Reporting & Conformance, a method for combatting phishing, was pioneered in the private sector and has become widespread in its use. Tokenization is another area led by private-sector standards. Tokenization involves replacing sensitive data with an alias (or token). Sensitive data is stored in a highly secure location and tokens are created to match the sensitive information. When information needs to be shared, only the token, not the sensitive information, is sent. Tokens can be created in real time and delivered securely over the internet, used for mobile device transactions, and securely shared between a wide variety of entities in the financial services ecosystem.

Several government-led initiatives on cybersecurity also exist. The US National Institute of Standards and Technology (NIST) created a Cybersecurity Framework in 2014, which it updated in 2018. Several other governments have used this standard as a model. The standard does not have a regulatory mandate but sets out best practices for industry.



The UK National Cyber Security Centre set up a minimum cybersecurity standard for its own departments.[89] Several international bodies, including the International Organization for Standardization, the Internet Engineering Task Force, the International Telecommunication Union and the Institute of Electrical and Electronics Engineers, have also produced standards related to cybersecurity.

The divergence in technical standards, interpretation and implementation creates challenges for entities looking to maintain high cybersecurity requirements and compliance. For instance, with authentication standards, multifactor authentication requires the presentation of at least two types of authentication elements, not just a PIN. A host of experiments in the public and private sectors are looking at such elements as location, type of device, fingerprint, user behaviour, iris scans and facial recognition. There is unanimous agreement that multifactor authentication is a cybersecurity best practice. In the private sector, the FIDO (Fast IDentity Online) Alliance is developing an open source standard for multifactor authentication, including biometrics. But divergence remains on regulation and government standards about what factors are valid methods of authentication. These divergences can create confusion for consumers and reduce security.

3.4 Recommendations: Best practices, initiatives and next steps

> Trust and security are paramount to the global payment system and nothing erodes trust more than breaches in security leading to fraud and cybercrime.

Trust and security are paramount to the global payment system and nothing erodes trust more than breaches in security leading to fraud and cybercrime. The solution to a world with increased threats due to technology is, perhaps paradoxically, more technology. Although cybersecurity is a well-known term, it is rarely understood. It encompasses more than the use of encryption technologies and best practices for authentication: cybersecurity requires robust internal security controls and best practices, ecosystem partnerships and public-private collaboration.

Although innovation and security do not always go hand in hand, the opportunity to address cyber-risks and to build cyber-resilience exists if carefully considered steps are taken by both the public and private sectors.

Establish public-private partnerships on cybersecurity

The Hewlett Foundation highlights the disconnect between technical practitioners and policy professionals as a major, persistent obstacle to the emergence of effective cybersecurity frameworks. The solution is to bring private-sector and academic technical experts together with policy experts in government.

Cybersecurity is a rapidly evolving field in which creating rigid regulatory standards could quell innovation and reduce security in the long term. The private sector should lead the development of new standards to combat emerging cyber-risks in cross-border payments. But the government should also play a key role, as part of a public-private partnership on standards development. It can endorse particular standards developed by the private sector through a non-binding set of recommendations.

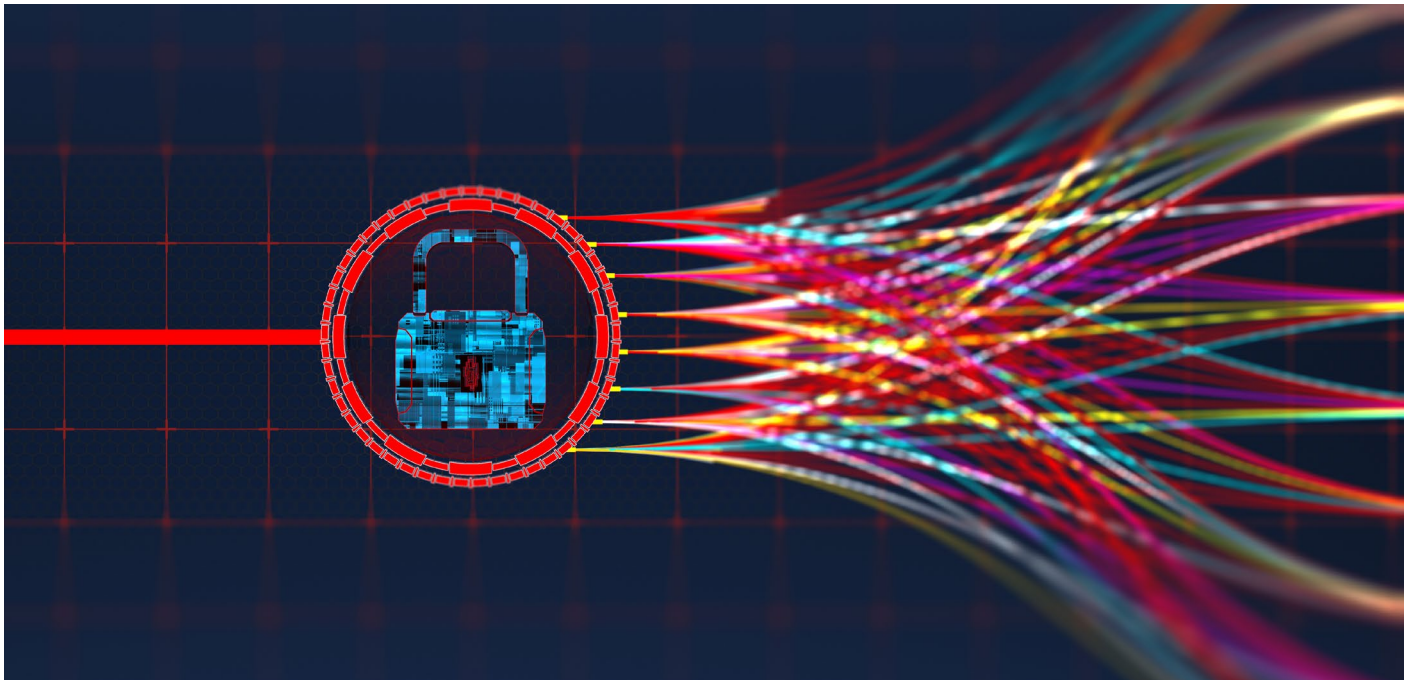
Encourage law enforcement cooperation and modernize mutual legal assistance treaties

A major cybersecurity concerns is law enforcement access to data, in particular in cross-border investigations. The current mutual legal assistance treaty-driven model is slow and onerous.

The US Clarifying Lawful Overseas Use of Data Act (or CLOUD Act) could provide a model framework. The first part of the act requires providers of electronic storage and communications to comply with US warrants for data physically housed in other countries. The second part authorizes executive agreements, such as the US-UK agreement, to allow a provider to share communications content with a qualifying foreign government.

The European Union has begun discussions on a potential CLOUD Act executive agreement and the United States and Australia formally announced negotiations as well. The CLOUD Act framework should be internationalized to create a more robust global framework for law enforcement data sharing. This, in turn, could encourage law enforcement agencies to cooperate on a broader set of issues, including identifying gaps in existing AML/CFT standards and other tax evasion practices.

The current CLOUD Act framework has certain limitations, namely the challenge for regulators and law enforcement agencies to gain access to data stored abroad by companies that have limited presence in-market. Thus far, developing countries have particularly struggled to gain access to data stored abroad and deserve special consideration.[90] The CLOUD Act framework allows for bilateral “executive agreements” between countries to obtain information stored abroad even without domestic presence in a market.



Further cooperation could also be encouraged through trade agreements, similar to provisions on e-commerce cooperation in the CPTPP.[91]

Encourage cyber hygiene through government-led programmes

The end user can be a major risk to the cyber ecosystem, and effective educational training could reduce cyber-risk globally. A well-informed customer is much less likely to be the victim of a cyberattack. Public-private partnerships will be essential to ensure that effective cybersecurity education reaches the end consumer.

“ Government-led campaigns to promote good cybersecurity practices have proven to be effective.

Improving the private sector’s capability of cyber defence should be another goal for government. Governments can set aside funding grants and hold competitions to incentivize innovation in the area of cybersecurity. The skills gap in the cybersecurity field is well known, but funding and support from government can help to improve the digital literacy and cyber hygiene of customers. Countries have set up “Innovation Academies” that gather industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organization leaders together to share practices and discuss regulatory and supervisory concerns with government representatives.

Greater cooperation between the industry and regulators is essential for the continued growth of the FinTech and RegTech sectors. For example, anti-phishing measures that can be promoted by governments include authentication standards that validate that the domain contained in an email “From” header is authentic by cross-checking against domain name system (DNS) records. Email servers can then accept, reject or warn against incoming emails based on this information. Financial institutions and payment providers are often used as bait in phishing attacks and have therefore developed expertise in countering them. By working closely with the private sector, governments can ensure that their constituents are better informed and protected against such attacks.

Government-led campaigns to promote good cybersecurity practices have also proven to be effective. In Singapore, for instance, eye-catching public service advisories in public transportation vehicles and stations provide public information about common cyberattacks, ways to prevent them and contact details of law enforcement agencies in case a user falls victim to a successful attack.

Work with the private sector to establish important consumer protections

The private sector must be diligent and careful in the way it engages with consumers regarding cybersecurity. Firms often make claims related to cybersecurity, and when the claims are found to be fraudulent, consumer protection litigation or regulation ensues. This type of regulation and litigation is legitimate, as false promises and fraud only serve to weaken the cybersecurity ecosystem.

Consumer protection concerns can also arise in relation to some of the other policy issues discussed above. The increase in data sharing with law enforcement, the monitoring of personal data to mitigate cyber-risk and the sharing of data between private entities to reduce cyber-risks can all trigger consumer protection issues, particularly pertaining to privacy. Policy-makers should work with the private sector to provide safe harbour privacy principles with regard to consumer protection regulation for data that is shared in good faith to reduce cyber-risk.

4

Innovation enabling oversight

Greater coordination is needed to improve competition and innovation

To ensure the safety and security of the financial sector, special regulatory consideration is given to payment service providers relative to other technology firms. When operating in multiple jurisdictions, companies may be subject to the supervisory requirements of multiple financial oversight bodies, which can lead to regulatory redundancies and inefficiencies and pose significant barriers to smaller firms that want to expand services across borders. These inefficiencies and market barriers in turn lower competition and increase the costs of cross-border payment services. This section explores ways that financial regulators can cooperate to reduce redundancies and friction in cross-border digital payments while ensuring adequate oversight.

4.1 Lack of international coordination on retail payment supervision

Financial regulators increasingly face the dilemma of encouraging innovation and greater competition among payment service providers while maintaining financial stability and a level playing field between firms. Supervisors want to offer FinTechs and new products and services regulatory flexibility and also ensure FinTechs are not circumventing necessary regulatory requirements or have an unfair advantage over existing payment service providers subject to robust regulation and oversight.

"New entrants may not have adequate resources to undergo examinations in multiple jurisdiction and thus may be unable to provide cross-border payment services in-market.

Historically, payment service regulators have taken a variety of approaches to oversight and supervision. In most jurisdictions, payment service providers, including FinTechs, are regulated with some degree of oversight but typically require less supervision than banking services more broadly, as payment services present less systemic risk to the financial system. For instance, in the United States, regulators oversee payment providers' processes and systems for managing a wide range of risks, from operational risk, to credit, liquidity, strategic, reputational, legal and compliance risks.[92] The level of regulatory oversight is typically in relation to how payment providers handle *e-money*, broadly defined as any electronic store of value that may be used for making payments.[93] Deposit holding presents greater financial-sector risk, so payment service providers holding deposits on behalf of customers are subject to greater regulatory oversight than providers only facilitating transactions between deposit holding accounts.[94]

The BIS's CPMI and the Board of the International Organization of Securities Commissions outline cooperation between regulators through the Principles for Financial Market Infrastructures (PFMI), specifically *Responsibility E: Cooperation with other authorities*. However, in practice, Responsibility E cooperation between regulatory entities has focused on systemically important market infrastructure, which often does not include retail payment systems because they pose significantly less risk than other clearing and settlement systems (e.g. securities exchanges, wholesale payment systems, etc.).

Despite a lack of international coordination and mutual recognition of supervisory requirements and licences from foreign jurisdictions, the approaches many countries take to payment system oversight are similar. Therefore, even if a firm meets oversight and supervision requirements in one jurisdiction, and these requirements are like those in other jurisdictions, that firm may still need to undergo additional examinations and licensing processes in every new jurisdiction in which it intends to provide services. This can be a significant barrier to firms, especially smaller firms, looking to provide cross-border payment services in multiple jurisdictions. Additionally, with higher barriers to entry come reduced competition and less availability of cross-border services. New entrants may not have adequate resources to undergo examinations in multiple jurisdiction and thus may be unable to provide cross-border payment services in-market.

4.2 Recommendations: Best practices, initiatives and next steps

To reduce barriers to entry and regulatory redundancy, greater international coordination between financial supervisors is necessary. Greater coordination will encourage information sharing and eliminate the need for redundant reporting and examination, and will lead to best practices for governing new financial technologies and products. Fortunately, recent bilateral and multilateral efforts to coordinate oversight and regulatory sandboxes for FinTechs provide examples of how countries can reduce oversight redundancies and streamline licensing for cross-border payment services.

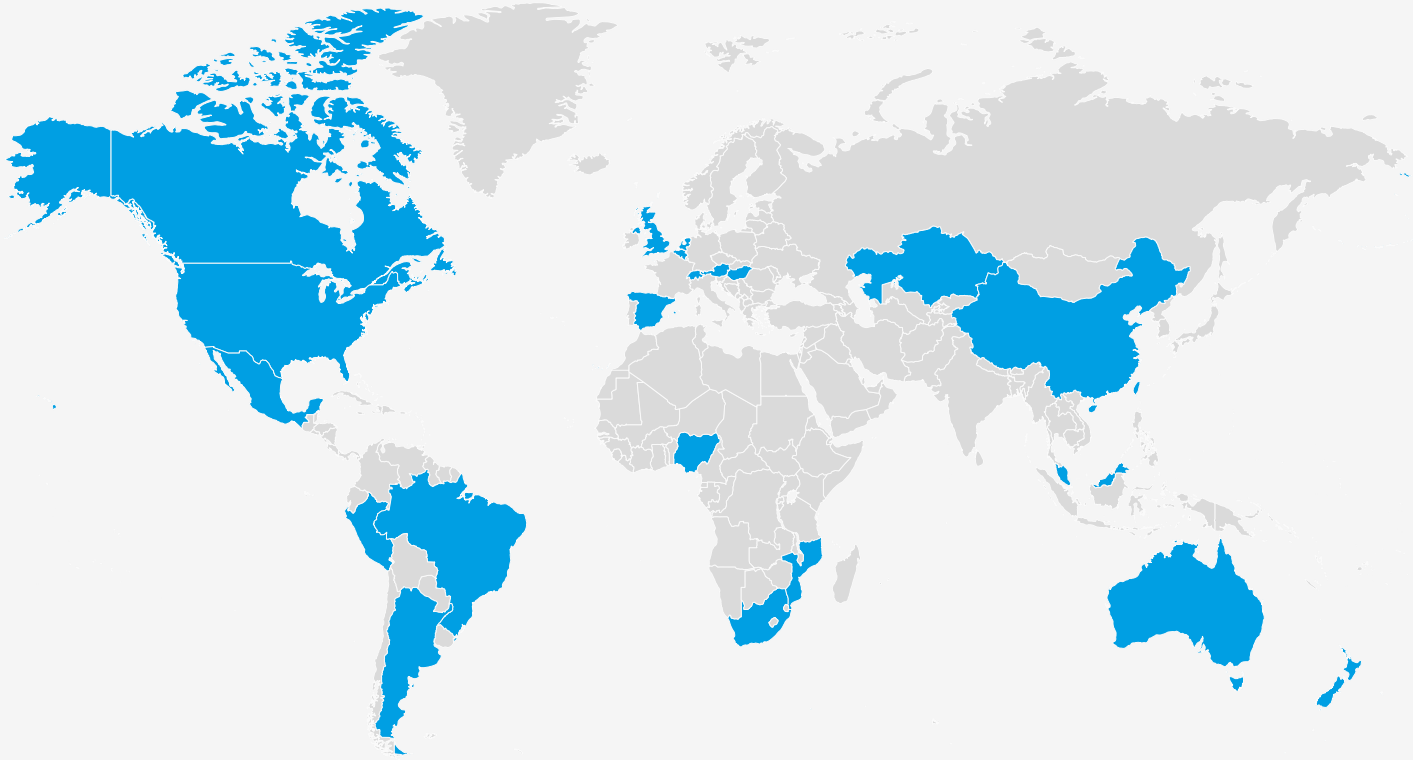
Explore bilateral, regional and multilateral oversight coordination

Many countries are entering into bilateral agreements to share information and improve the coordination of regulatory oversight for firms providing cross-border financial services, including payments. Singapore again provides a good model of international cooperation on cross-border payment services. Since 2016, the MAS has signed 33 FinTech Cooperation Agreements with its regulatory oversight counterparts in jurisdiction around the world.[95] These cooperation agreements vary in scope but tend to focus on three areas: information sharing between regulatory authorities, referral of qualified firms to other jurisdictions, and commitments to explore joint projects related to financial innovation.

Each of these types of commitments reduces inefficiencies in cross-border licensing and oversight requirements while ensuring regulatory supervision. For example, a 2017 Cooperation Agreement between the MAS and the Hong Kong Monetary Authority (HKMA) allows for FinTechs meeting oversight requirements in one jurisdiction to be referred to the other.[96] The agreement also formalizes information sharing between both supervisory authorities – regarding specific firms operating in both jurisdiction and the broader sharing of best practices – with the intent to "create significant synergy for the development of FinTech and more efficient fund flows between the two markets".[97]

More recently, several supervisory authorities have moved to multilateral coordination of FinTech oversight, including for cross-border payment service providers, through the Global Financial Innovation Network (GFiN). Supervisory authorities with regulatory sandboxes for FinTech came together in 2018 to form the GFiN to share best practices. Since then, the goal of the GFiN has evolved, with two main objectives: 1) to provide FinTechs with a more efficient way to work with regulators; and 2) to improve cross-border coordination between financial authorities.[98] In just over a year, GFiN has expanded its network (Figure 2) to over 43 financial system regulators, representing prominent national and subnational agencies leading sandbox efforts.[99] GFiN is also open to accepting non-regulatory observing members, including groups such as the World Bank, the International Monetary Fund (IMF), the Consultative Group to Assist the Poor (CGAP) and other development finance institutions.

FIGURE 2 **GFiN member locations**



Source: Consultative Group to Assist the Poor (CGAP), "Global Financial Innovation Network: Not Global Yet", 14 November 2018, https://www.cgap.org/blog/global-financial-innovation-network-not-global-yet

Beyond coordinating domestic FinTech sandbox programmes, GFiN also recognizes the importance of greater regulatory cooperation specifically for cross-border financial services, including retail payments. In 2019, GFiN launched a cross-border testing pilot for FinTechs focused on providing cross-border services, which included payment service providers.[100] While this pilot was limited in scope with just eight firms selected for inclusion, the lessons learned led to several useful tools that could potentially improve cross-border payment services. They include the creation of a *regulatory compendium* that identifies the types of activities regulators in different countries can support, a helpful tool for firms that want to provide cross-border payment services.[101] Additionally, GFiN is currently developing a common application across jurisdictions to streamline cross-border service pilots for FinTechs.[102]

GFiN's successes during its first year of operation present an opportunity to expand its scope beyond regulatory sandboxes to financial technology providers more broadly, and specifically to other cross-border payment service providers. While it is important to support the entrance of new technology providers, it is also important to maintain a level playing field with established cross-border service providers who already bear significant costs for regulatory oversight in each jurisdiction. Expanded cooperation could be facilitated through the existing network or through the creation of a new network with specific focus on streamlining retail payment oversight. The emphasis of such a group would be more on coordination and licensing referral and less on standards, which are largely under the purview of the CPMI.[103]

In addition, moving one step beyond cross-border coordination, countries could do more than share regulatory information and adopt regulatory "passports" for FinTechs. Currently within the European Union, payment operators licensed in one member state can passport these licences into other member states in accordance with EU financial services Directives.[104] With the UK leaving the European Union, UK negotiators are exploring how to continue this arrangement with EU members and potentially expand it to other countries outside of Europe.[105] Assuming sufficient coordination between regulators and risk mitigation, passporting is a natural progression towards streamlining oversight and licensing requirements and could make it significantly easier to bring FinTechs to scale and offer cross-border services.

Conclusion

Addressing cross-border payments requires a holistic approach

Facilitating cross-border retail payments today requires connections between a complex set of banks, applications, domestic and international payment service providers and, of course, consumers and merchants. As outlined in this report, significant work to improve cross-border payment efficiency is needed, but many innovative policy-makers and companies are working together to chart a way forward.

The four areas of focus for policy-makers highlighted in this report are interdependent and should, therefore, be addressed in harmony. Without addressing market barriers and data restrictions, international firms cannot bring cross-border services to market, and it is even more difficult for new, domestically focused entrants to scale by expanding abroad and forming partnerships with international firms. Without improving interoperability between payment service providers, the friction in making connections between countries and networks will only increase as more providers enter the market. Without addressing security and trust in cross-border payments, cyberattacks and fraud will disrupt commerce across borders. Finally, without adequate oversight and cooperation among financial system supervisors, competition and financial stability in payment services will suffer.

This report has primarily focused on facilitating cross-border retail payments, but addressing policy challenges in these four areas is critical to other issues facing payments domestically. The World Economic Forum will explore many of these topics in its research, particularly those pertaining to financial inclusion and the role of digital currencies in the future of payments. Examining these challenges will be particularly important for current crises, where gaps in financial inclusion and digital readiness have been laid bare by the shift away from in-person commerce to e-commerce.

This report aims to offer practical, holistic solutions to strengthen both the efficiency and inclusiveness of economies by addressing a number of practical governance challenges in parallel. Public-private cooperation is needed more than ever as the digital transformation of the global economy accelerates at an unprecedented rate.

Contributors

In drafting this report, the World Economic Forum took a multistakeholder approach to convene a global community of industry leaders, policy-makers, members of academia and civil society from various jurisdictions, and representatives of international organizations.

Lead authors

Mike Gallaher
Director, Public Policy, Visa, USA; Fellow, Digital Trade, World Economic Forum LLC

Nigel Cory
Associate Director, Trade Policy, Information Technology and Innovation Foundation (ITIF), USA

Usman Ahmed
Head, Global Public Policy, PayPal, USA

The Forum thanks the following contributors for their support and expertise since the establishment of the Cross-Border Digital Payments Portfolio.

Nick Ashton-Hart
Geneva Representative, Digital Trade Network, Switzerland

Isabella Ali Pontual Braga
Associate, Cescon Barrieu, Brazil

Sahra English
Vice-President, Global Policy, MasterCard, USA

Antonia Esser
Senior Associate, Cenfri, South Africa

May-Ann Lim
Executive Director, Asia Cloud Computing Association, Singapore

Mabel Lyu
Senior Adviser, Rules and Standards Management, Ant Financial Services Group, People's Republic of China

Martin Molinuevo
Senior Counsel, World Bank Group, Washington DC

Laura Munoz Perez
Senior Engagement Manager, Cenfri, South Africa

Harish Natarajan
Lead Financial Sector Specialist on Payments and Market Infrastructures, World Bank, Washington DC

Raoul Renard
Government Affairs Manager, International Chamber of Commerce (ICC), France

Mauricio Santos
Founding Partner, Cescon Barrieu, Brazil

Geoffrey See
General Manager and Head of Identity, Trusting Social, Singapore

Tan Nyat Chuan
Senior Director, Payments Market ASEAN, SWIFT, Malaysia

Alexandre Trejos Vargas
Associate, Cescon Barrieu, Brazil

Arun Venkataraman
Senior Director, Global Government Engagement, Visa, USA

Grace Wu
Head, Risk Partnership, Uber, USA

World Economic Forum

Kimberley Botwright
Community Lead, International Trade and Investment

Sean Doherty
Head, International Trade and Investment

Ziyang Fan
Head, Digital Trade, World Economic Forum LLC

Ashley Lannquist
Project Lead, Blockchain and Digital Currency, World Economic Forum LLC

Jesse Lin
Project Specialist, Digital Trade, World Economic Forum LLC

Drew Propson
Head, Technology and Innovation in Financial Services, World Economic Forum LLC

Yan Xiao
Project Lead, Digital Trade, World Economic Forum LLC

Endnotes

1. Moody's Analytics, *The Impact of Electronic Payments on Economics Growth*, 2016, https://usa.visa.com/dam/VCOM/download/visa-everywhere/global-impact/impact-of-electronic-payments-on-economic-growth.pdf; Kearny, "Digital payments and the global informal economy", 2018, https://www.kearney.com/financial-services/digital-payments-and-the-global-informal-economy.
2. Moody's Analytics, *The Impact of Electronic Payments on Economics Growth*, op. cit.
3. World Economic Forum, "Addressing E-Payment Challenges in Global E-Commerce", White Paper, 2018, http://www3.weforum.org/docs/WEF_Addressing_E-Payment_Challenges_in_Global_E-Commerce_clean.pdf.
4. Bolt, Wilko, and Sujit Chakravorti, "Digitization of Retail Payments", De Nederlandsche Bank Working Paper, No. 270, 2010, https://www.dnb.nl/binaries/Working%20paper%20270_tcm46-243674.pdf.
5. Asia-Pacific Economic Cooperation (APEC), *Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses*, Chapter 4: Payment Services, 2019, https://www.apec.org/-/media/APEC/Publications/2019/7/Fostering-an-Enabling-Policy-and-Regulatory-Environment-in-APEC-for-Data-Utilizing-Businesses/TOC/Chapter-4.pdf.
6. WTO, China – *Certain Measures Affecting Electronic Payment Services: Report of the Panel*, WT/DS413/R, 16 July 2012, para. 7.99, pp. 35-36.
7. World Economic Forum, "Addressing E-Payment Challenges in Global E-Commerce", op. cit.
8. Ibid.; The "EU15" countries are counted as one WTO member; 22 members have full market access commitments and 31 have partial market access commitments on payment and money transmission services.
9. International Chamber of Commerce, "Electronic payment services and e-commerce", ICC Issues Brief No. 4, 2020, https://iccwbo.org/content/uploads/sites/3/2020/02/icc-issues-brief-4-electronic-payment-services-and-ecommerce.pdf.
10. Central Bank of Nigeria, *Guidelines on Point of Sale (POS) Card Acceptance Services*, August 2011, http://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf.
11. Dentons, "Banking and Finance, Major Russian Legislation Changes for 2016, Regulation of the payment sector", 2 March 2017, https://www.dentons.com/en/insights/alerts/2017/march/2/major-russian-legislation-changes-for-2016-banking-and-finance#4; Dentons, Federal Law No. 161-FZ "On the National Payment System", 27 June 2011 (the NPS Law) as amended in October 2014 by Federal Law No. 319-FZ "On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation", https://www.dentons.com/en/insights/alerts/2014/november/11/international-payment-cards-processing-from-russia-with-love; National Payment Card System (NSPK), "Russian National Payment Card System", https://nspk.com/.
12. Bank Indonesia, Payment System, "Regulation of Bank Indonesia No. 19/8/PBI/2017 on National Payment Gateway", 1 November 2017, https://www.bi.go.id/en/peraturan/sistem-pembayaran/Pages/pbi_190817.aspx; Information Technology Industry Council, "Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses", 2017, https://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf.
13. American Chamber of Commerce in Hanoi (AmCham), "Vietnam: Trade Summary", http://www.amchamhanoi.com/wp-content/uploads/2018/04/NTE-vietnam-2018.pdf.
14. APEC, *Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses*, Chapter 4: Payment Services, op. cit.
15. World Economic Forum, "Addressing E-Payment Challenges in Global E-Commerce", op. cit.
16. Meltzer, Joshua, and Peter Lovelock, *Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia*, Brookings, 2018, https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/; Cory, Nigel, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", Information Technology & Innovation Foundation, 1 May 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
17. Manyika, James, et al., "Digital globalization: The new era of global flows", McKinsey Global Institute, 24 February 2016, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.
18. Thaker, Aria, "India's data localisation plans could hurt its own startups the most", *Quartz India*, 16 October 2018, https://qz.com/india/1422014/rbis-data-localisation-could-hurt-indias-own-startups/.
19. APEC, *Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses*, Chapter 4: Payment Services, op. cit.
20. Bankacilik Düzenleme ve Denetleme Kurumu (BDDK), Turkish Banking Regulation and Supervision Agency, "Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions", Law No. 6493 of 20 June 2013, *Official Gazette*, Issue No. 28690, 27 June 2013, https://www.bddk.org.tr/ContentBddk/dokuman/mevzuat_0140.pdf.

21. Lunden, Ingrid, "PayPal to halt operations in Turkey after losing license, impacts 'hundreds of thousands'", TechCrunch, 31 May 2016, https://techcrunch.com/2016/05/31/paypal-to-halt-operations-in-turkey-after-losing-license-impacts-hundreds-of-thousands/.

22. Reserve Bank of India, Notifications, "Storage of Payment System Data", 6 April 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11244.

23. Reserve Bank of India, Frequently Asked Questions, "Storage of Payment System Data", 2018, https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130.

24. Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel and Bert Verschelde, "Data Localisation in Russia: A Self-imposed Sanction", European Centre for International Political Economy (ECIPE), Policy Brief, 2015, https://ecipe.org/wp-content/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.

25. Atkinson, Robert, and Nigel Cory, "ITIF Filing to the Central Bank of Brazil on Cybersecurity and Data Processing Requirements", Information Technology & Innovation Foundation, 14 November 2017, https://itif.org/publications/2017/11/14/itif-filing-central-bank-brazil-cybersecurity-and-data-processing.

26. For examples, see Bank of Ghana, "Payment Systems and Services Act, 2019", Act 987, 12 June 2019, https://www.bog.gov.gh/wp-content/uploads/2019/08/Payment-Systems-and-Services-Act-2019-Act-987-.pdf; Perez, Sarah, "Mastercard given approval to prepare for entry into China's payments market", TechCrunch, 11 February 2020, https://techcrunch.com/2020/02/11/mastercard-given-approval-to-prepare-for-entry-into-chinas-payments-market/; Baker McKenzie, "Vietnam: Proposed Cap on Foreign Ownership on Intermediary Payment Services Companies", 29 November 2019, https://www.bakermckenzie.com/en/insight/publications/2019/11/foreign-ownership-intermediary-payment-services.

27. Bank of Ghana, "Payment Systems and Services Act, 2019", op. cit.

28. Bank Indonesia, Payment System, "Regulation of Bank Indonesia No. 19/8/PBI/2017 on National Payment Gateway", op. cit.

29. World Economic Forum, "Addressing E-Payment Challenges in Global E-Commerce", op. cit.

30. WTO, "General Agreement on Trade in Services, Article XVII: National Treatment", https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXVII.

31. WTO, "Understanding on commitments in financial services", https://www.wto.org/english/tratop_e/serv_e/21-fin_e.htm. For example, a measure that bans the cross-border electronic transmission of data that constitutes the service being supplied in a committed service (i.e. provision and transfer of financial information and financial data processing as referred to in subparagraph 5(a)(xv) of the Annex on Financial Services) would be inconsistent with relevant market access commitments.

32. WTO, *Mexico – Measures Affecting Telecommunications Services: Report of the Panel*, WT/DS204/R, 2 April 2004, para. 7.45.

33. WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services: Report of the Panel*, WT/DS285/R, 10 November 2004, para. 6.281.

34. WTO, GATS "Annex on financial services, 5. Definitions". The scope of these services was addressed by a dispute settlement panel in the case of *China – Certain Measures Affecting Electronic Payment Services*, which defined the sector broadly.

35. Subject to exception provisions in the agreement.

36. Provision and transfer of financial information and financial data processing as referred to in subparagraph 5(a)(xv) of the Annex on Financial Services.

37. Crosby, Daniel, "Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments", E15 Initiative, 2016. See also Tuthill, L. Lee, "Cross-border data flows: What role for trade rules?", in Pierre Sauvé and Martin Roy (eds), *Research Handbook on Trade in Services*, Edward Elgar, 2016.

38. WTO, "Annex on telecommunications, 5. Access to and use of Public Telecommunications Transport Networks and Services", in which paragraph 5c states: "Each Member shall ensure that service suppliers of any other Member may use public telecommunications transport networks and services for the movement of information within and across borders, including for intra-corporate communications of such service suppliers, and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of any Member. Any new or amended measures of a Member significantly affecting such use shall be notified and shall be subject to consultation, in accordance with relevant provisions of the Agreement".

39. Financial institutions are not "covered persons" in this chapter.

40. Government of Canada, "Consolidated TPP Text – Chapter 11 – Financial Services, Annex 11-B, Section B: Transfer of Information", https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/11.aspx?lang=eng.

41. See Articles 17.17 and 17.18 of the USMCA trade agreement, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/17-Financial-Services.pdf.

42. Ibid., see Articles 17.3.3 and 17.5.1. The parties agree not to cap the number of electronic payment service suppliers, limit the value of transactions or assets, apply economic needs tests, restrict the number of employees or limit the types of legal entities through which firms can offer their electronic payment services.

43. Ibid., see Article 17.18.

44. Ibid.

45. Ibid.; APEC, *Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses*, Chapter 4: Payment Services, op. cit. Furthermore, even were a regulator to have concerns about access to data, the countries agreed to provide financial firms with a reasonable opportunity to make changes to their IT systems (i.e. shifting data storage from one jurisdiction or another) without necessarily shifting data to a regulator's jurisdiction (e.g. another third-country jurisdiction where regulators know they would have requisite access).

46. The adoption of the Reference Paper principles by a large majority of participants in the WTO negotiations on basic telecommunications in 1997 was – and remains – one of the major achievements of the WTO to date. It was the first move by countries to take additional commitments in the GATS. At a time when many economies were making the transition from a monopoly-based to a market-based model in telecommunications, the Reference Paper proved instrumental in supporting the successful introduction of competition and in enabling the telecommunications sector to grow on a sound basis. See WTO, "Negotiating group on basic telecommunications", Telecommunications Services Reference Paper, 24 April 1996, https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

47. See "Consolidated TPP Text – Chapter 11 – Financial Services, Article 11.7: New Financial Services".

48. Monetary Authority of Singapore, "MAS Establishes Payments Council", Press release, 2 August 2017.

49. Banco Central Do Brasil, "Instant Payments/Permanent 'IP Forum'", https://www.bcb.gov.br/en/financialstability/instantpayments.

50. HSBC, "Payments in ASEAN post AEC", Hongkong and Shanghai Banking Corporation Limited, 2014, https://skm.hsbc.com.my/1/PA_ES_Content_Mgmt/content/website/commercial/cash_management/PDF_141107/5-Payments-in-ASEAN-post-AEC.pdf.

51. World Economic Forum, "Digital ASEAN", 2018, https://www.weforum.org/projects/digital-asean.

52. Benson, Carol C., and Scott Loftesness, *Interoperability in Electronic Payments: Lessons and Opportunities*, Consultative Group to Assist the Poor (CGAP), 2012, https://www.cgap.org/sites/default/files/researches/documents/Interoperability_in_Electronic_Payments.pdf.

53. Seth, Shobhit, "How the SWIFT System Works", Investopedia, 11 February 2020, https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp.

54. Bank for International Settlements (BIS), *Report on open banking and application programming interfaces*, November 2019, https://www.bis.org/bcbs/publ/d486.pdf.

55. The Paypers, *Open Banking Report 2019 - Insights into the Global Open Banking Landscape*, September 2019, https://thepaypers.com/reports/the-open-banking-report-2019-insights-into-the-global-open-banking-landscape-2/r780814.

56. BIS, *Report on open banking and application programming interfaces*, op. cit.

57. Ibid.

58. Based on the FATF's global evaluation of countries' compliance with FATF Recommendations 2012 and Methodology 2013; see the Fourth Round Ratings, http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf.

59. See the FATF's consolidated ratings particularly regarding Recommendation 10 on customer due diligence, Recommendation 13 on correspondent banking, Recommendation 16 on wire transfers, and Immediate Outcome 4 on the application of preventive measures by regulated entities.

60. Bank for International Settlements (BIS), *Cross-border retail payments*, February 2018, https://www.bis.org/cpmi/publ/d173.pdf.

61. New Zealand Ministry of Foreign Affairs and Trade, "Digital Economy Partnership Agreement ("DEPA") Between Singapore, Chile & New Zealand, Article 2.7: Electronic Payments", 21 January 2020, https://www.mfat.govt.nz/assets/FTAs-agreed-not-signed/DEPA/DEPA-Chile-New-Zealand-Singapore-21-Jan-2020-for-release.pdf.

62. Ibid., p. 11.

63. Rothwell, Graham, "The Brave New World of Open Banking in APAC: Singapore", Accenture, 27 September 2018, https://bankingblog.accenture.com/brave-new-world-open-banking-apac-singapore.

64. See the comprehensive list at Monetary Authority of Singapore, "Financial Industry API Register", 2020, https://www.mas.gov.sg/development/fintech/financial-industry-api-register.

65. Thaker, "India's data localisation plans could hurt its own startups the most", op. cit.

66. Chen, Greg, and Xavier Faz, "Open Data and the Future of Banking", Consultative Group to Assist the Poor (CGAP), 23 October 2019, https://www.cgap.org/blog/open-data-and-future-banking.

67. Bank for International Settlements (BIS), *Fast payments – Enhancing the speed and availability of retail payments*, November 2016, https://www.bis.org/cpmi/publ/d154.pdf.

68. FIS Financial Solutions, *Flavors of Fast*, 2019, https://www.fisglobal.com/flavors-of-fast; summary article: Finextra, "FIS: 54 countries have activated real-time payment systems", 19 September 2019, https://www.finextra.com/pressarticle/79917/fis-54-countries-have-activated-real-time-payment-systems.

69. ISO 20022 [website], "A single standardisation approach (methodology, process, repository) to be used by all financial standards initiatives", https://www.iso20022.org/.

70. See ISO, "ISO 8583-1:2003(en)" for more information, https://www.iso.org/obp/ui/#iso:std:iso:8583:-1:en.

71. World Economic Forum, "ASEAN e-Payments Coalition: e-Payments Recommendation Paper", Digital ASEAN Initiative, 2019, https://weforum.ent.box.com/v/epaymentsrecommendationpaper.

72. Rashid, Naeha, and Stefan Staschen, "Unlocking Financial Inclusion Using Biometrically Verified SIMs", Consultative Group to Assist the Poor (CGAP), 26 July 2016, www.cgap.org/blog/unlocking-financial-inclusion-using-biometrically-verified-sims.

73. Alliance for Financial Inclusion (AFI), *KYC Innovations, Financial Inclusion and Integrity In Selected AFI Member Countries*, 2019, https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf.

74. Monetary Authority of Singapore, "Singapore and Kenya Establish Cooperation on Developing Digital Infrastructure at Inaugural Afro-Asia FinTech Festival", Press release, 17 July 2019, https://www.mas.gov.sg/news/media-releases/2019/singapore-and-kenya-establish-fintech-cooperation-at-inaugural-afro-asia-fintech-festival.

75. Hota, A.P., "One nation, under code: How India leads the way in the interoperability of QR code for payments", *The Economic Times*, 8 October 2017, https://economictimes.indiatimes.com/industry/banking/finance/banking/one-nation-under-code-how-india-leads-the-way-in-the-interoperability-of-qr-code-for-payments/articleshow/60986772.cms.

76. World Economic Forum, "ASEAN e-Payments Coalition: e-Payments Recommendation Paper", op. cit.

77. Association of Southeast Asian Nations (ASEAN), *ASEAN Economic Community Blueprint 2025*, 2015, https://www.asean.org/storage/2016/03/AECBP_2025r_FINAL.pdf.

78. World Economic Forum, "ASEAN e-Payments Coalition: e-Payments Recommendation Paper", op. cit., p. 6.

79. See BIS, "Innovation and fintech: The future of central banking is inextricably linked to innovation", https://www.bis.org/topic/fintech.htm; EMVCo [website], https://www.emvco.com/.

80. PwC, "Consumer Intelligence Series: Protect.me", September 2017, https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf.

81. Bricata, "10 Statistics that Summarize the State of Cybersecurity in Financial Services", Security Boulevard, 12 November 2019, https://securityboulevard.com/2019/11/10-statistics-that-summarize-the-state-of-cybersecurity-in-financial-services/.

82. Lewis, James, *Economic Impact of Cybercrime – No Slowing Down*, Center for Strategic & International Studies (CSIS), 21 February 2018, https://www.csis.org/analysis/economic-impact-cybercrime.

83. Mazars, "Global Ecommerce Survey 2017", 2017, https://www.mazars.com/Home/News-and-Insights/Our-publications/Surveys-and-studies/Global-Ecommerce-Survey-2017.

84. GSM Association (GSMA), "The Mobile Economy 2020", March 2020, https://www.gsma.com/r/mobileeconomy/.

85. Chapman, Tom, "Spear-Phishing Could Enable Cyberterrorism Attacks Against The U.S.", TechCrunch, 27 March 2015, https://techcrunch.com/2015/03/27/spear-phishing-could-enable-cyberterrorism-attacks-against-the-u-s/.

86. Barker, Ian, "Cost of an enterprise data breach rises to $1.41 million", betanews, 1 October 2019, https://betanews.com/2019/10/01/enterprise-data-breach-cost/.

87. Stanford Center on Longevity, FINRA Investor Education Foundation and BBB Institute for Marketplace Trust, *Exposed to Scams – What Separates Victims from Non-Victims?*, 2019, http://longevity.stanford.edu/wp-content/uploads/2019/09/ScamTrackerIssueBrief-ExposedToScamsReducedFile.pdf.

88. Ponemon Institute, *2018 State of Cybersecurity in Small & Medium Size Businesses*, 2018, https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf.

89. United Kingdom Cabinet Office, "Minimum Cyber Security Standard", 25 June 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf.

90. Molinuevo, Martin, and Simon Gaillard, "Trade, Cross-Border Data, and the Next Regulatory Frontier: Law Enforcement and Data Localization Requirements", World Bank Group, 2018, http://documents.worldbank.org/curated/en/903261543589829872/Trade-Cross-Border-Data-and-the-Next-Regulatory-Frontier-Law-Enforcement-and-Data-Localization-Requirements.

91. Ibid.

92. Federal Financial Institutions Examination Council (FFIEC), "Retail Payment Systems Risk Management", https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management.aspx; *Retail Payment Systems IT Examination Handbook*, 2016, https://ithandbook.ffiec.gov/media/274860/ffiec_itbooklet_retailpaymentsystems.pdf.

93. Bank for International Settlements (BIS), *Policy responses to fintech: a cross-country overview*, Financial Stability Institute (FSI) Insights on policy implementation No. 23, January 2020, https://www.bis.org/fsi/publ/insights23.pdf.

94. Ibid.

95. Monetary Authority of Singapore, "FinTech Cooperation Agreements", February 2020, https://www.mas.gov.sg/development/fintech/fintech-cooperation-agreements.

96. Hong Kong Monetary Authority, "Fintech Collaboration between the Hong Kong Monetary Authority and the Monetary Authority of Singapore", Press release, 25 October 2017, https://www.hkma.gov.hk/eng/news-and-media/press-releases/2017/10/20171025-4.

97. Ibid.; quote from Norman Chan, Chief Executive of the HKMA.

98. Global Financial Innovation Network, "About GFiN", 2019, https://www.thegfin.com/about.

99. Global Financial Innovation Network, "Our Members", February 2020, https://www.thegfin.com/members.

100. They included a distributed ledger company (DACX) with payment capabilities, which was accepted as one of the eight firms selected for the pilot. See GFiN, *Cross-Border Testing: Lessons Learned*, January 2020, https://www.cbb.gov.bh/wp-content/uploads/2020/01/GFIN-CBT-Pilot-lessons-Learned-publication.pdf.

101. Global Financial Innovation Network, "GFiN Regulatory Compendium", February 2020, https://www.thegfin.com/compendium-1.

102. Global Financial Innovation Network, *Cross-Border Testing: Lessons Learned*, op. cit.

103. See BIS, "Principles for Financial Market Infrastructures (PFMI)", February 2020, https://www.bis.org/cpmi/info_pfmi.htm.

104. Sidley Austin LLP, "Brexit Implementation Period and Beyond: Key Points for the Payments Sector", 28 January 2020, https://www.sidley.com/en/insights/newsupdates/2020/01/brexit-implementation-period-and-beyond_key-points-for-the-payments-sector.

105. Digalaki, Eleni, "UK lawmakers are eyeing post-Brexit passporting beyond Europe", Business Insider, 28 January 2019, https://www.businessinsider.com/uk-treasury-eyes-post-brexit-financial-service-passporting-2019-1.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org