WP/20/75

IMF Working Paper

Fintech and Payments Regulation: Analytical Framework

by Tanai Khiaonarong and Terry Goh

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

INTERNATIONAL MONETARY FUND

© 2020 International Monetary Fund

IMF Working Paper

Monetary and Capital Markets Department

Fintech and Payments Regulation: Analytical Framework

Prepared by Tanai Khiaonarong and Terry Goh*

Authorized for distribution by Jihad Alwazir

May 2020

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

Disclaimer: This document was prepared before COVID-19 became a global pandemic and resulted in unprecedented economic strains. It, therefore, does not reflect the implications of these developments and related policy priorities. We direct you to the **IMF Covid-19 page** that includes staff recommendations with regard to the COVID-19 global outbreak.

Abstract

Financial technology (Fintech) has prompted authorities to consider their potential financial stability benefits, risks, and effective regulation. Recent developments suggest that regulatory approaches and their legal foundations need to augment entity-based regulation with increasing focus on activities and risks as market structure changes. This paper draws on recent international experiences in modernizing legal and regulatory frameworks for payment services. An analytical framework based on a four-step process is proposed—(i) identifying payment activities; (ii) licensing entities and designating systems; (iii) analyzing and managing risks, and (iv) promoting legal certainty. As payment activities evolve and potential systemic risks heighten, adherence to international standards and additional regulatory requirements should be warranted.

JEL Classification Numbers: E42 E58 E59 G28 K20 O38

Keywords: Fintech, payment services, central bank, regulation

Author's E-Mail Address: tkhiaonarong@imf.org; terrygohph@gmail.com

*Terry Goh was formerly with the Monetary Authority of Singapore. We thank Wouter Bossu, Jess Cheng, Simon Gray, Dong He, Kathleen Kao, Aditya Narain, Harish Natarajan, Kristel Poh, Alexandre Stervinou, Jan Vermeulen for helpful comments and suggestions. An earlier version was presented at the Joint European Central Bank—National Bank of Belgium Retail Payments Conference in Brussels on November 27, 2019. Karen Lee helped with research and Wifianni Wirsatyo provided editorial assistance.

Contents Page

Boxes

Appendix

GLOSSARY

AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Authorized Payment Institution
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CBR	Correspondent Banking Relationship
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
EC	European Commission
ELMI	Electronic Money Institution (in the European Union)
EMI	Electronic Money Institution (in the United Kingdom)
EU	European Union
EUR	Euro
FATF	Financial Action Task Force
FINMA	Swiss Financial Market Supervisory Authority
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
GSC	Global Stablecoin
GSMA	Groupe Speciale Mobile Association
IADI	International Association of Deposit Insurers
ICO	Initial Coin Offering
IMF	International Monetary Fund
ML	Machine Learning
MNO	Mobile Network Operator
MPI	Major Payment Institution (in Singapore)
ORPS	Other Retail Payment Systems
OTC	Over the Counter
PFMI	Principles for Financial Market Infrastructures
PI	Payment Institution
PIRPS	Prominently Important Retail Payment Systems
PPS	Postal Payment Service
PS Act	Payment Services Act of Singapore
PSD2	Payment Services Directive 2 of the European Union
PSP	Payment Service Provider
SGD	Singapore Dollar
SIPS	Systemically Important Payment System
SPI	Standard Payment Institution (in Singapore)
SPI	Small Payment Institution (in the United Kingdom)
SWIPS	System-Wide Important Payment Systems
TA	Technical Assistance
UNCITRAL	United Nations Commission on International Trade Law
VA	Virtual Asset
VASP	Virtual Asset Service Provider

I. MOTIVATION FOR ANALYTICAL FRAMEWORK

Financial technology (Fintech) has prompted authorities to consider their potential financial stability benefits, risks, and effective regulation.[1] Payments, clearing and settlements is one area where material fintech developments and experimentations have rapidly evolved. This spans across large-value, retail, and cross-border payments. Changes in the retail payment services landscape is among the most visible so far. Motivations have been varied, including promoting cashless-ness, competition, financial inclusion, financial integration, and innovation to addressing correspondent banking relationship (CBR) withdrawals (IMF, 2017). While there are no compelling financial stability risks given the small size of fintech relative to the financial system, growth in such activities and the supervisory and regulatory issues have merited authorities' attention (IMF, 2019; FSB, 2017a).

Authorities regulate payment systems and payment service providers (PSPs) for many reasons. They include: to maintain the integrity of the monetary system, safeguard financial stability by ensuring final settlement of monetary transfers, and protect consumers with regards to non-currency money (commercial bank book money and e-money) that entail credit risks. Fintech's impact on financial stability may also change quickly with the market entrance and expansion of large technology firms into payment services.

Fintech developments suggest that regulatory approaches and their legal foundations need to augment entity-based regulation with increasing focus on activities-based approaches, as market structure changes. Financial regulation has been traditionally based on the regulation of types of entities or intermediaries performing broad functions such as payment systems (He et al., 2017). Licensing regimes will need to be redesigned to bring new types of service providers within the regulatory perimeter, where appropriate, including fintech and large technology firms, or Big Tech (BIS, 2019; FSB, 2019a; Frost et al., 2019; Restoy, 2019).

Some jurisdictions have modernized their legal and regulatory framework for payment services, using an activity-based and risk-focused approach.[2] Modernization efforts have aimed to foster safety, efficiency, innovation and competition. New business models for payment services have blurred the lines of payment related products that may for example, require licensing as an electronic money issuer and a money remittance business, leading to overlapping regulation; or gaps in regulation if the product is licensed as one but not the other. In modernizing the oversight framework, there is thus a need to align relevant

[1] The Bali Fintech Agenda proposed a framework that focused on 12 relevant elements, including financial sector resilience, risks, and international cooperation (IMF/World Bank, 2018). Payments and settlement systems, and central bank digital currency were among the key issues identified as meriting further attention (IMF/World Bank, 2019).

[2] For illustration, this has included the European Union and Singapore. Canada has also initiated reforms to the oversight framework for retail payments (Department of Finance Canada, 2019).

regulations and amend the scope of regulated activities to facilitate new business models and payment entities. At the same time, these new business models present emerging risks which may not be addressed, or adequately addressed, under current regulatory regimes.

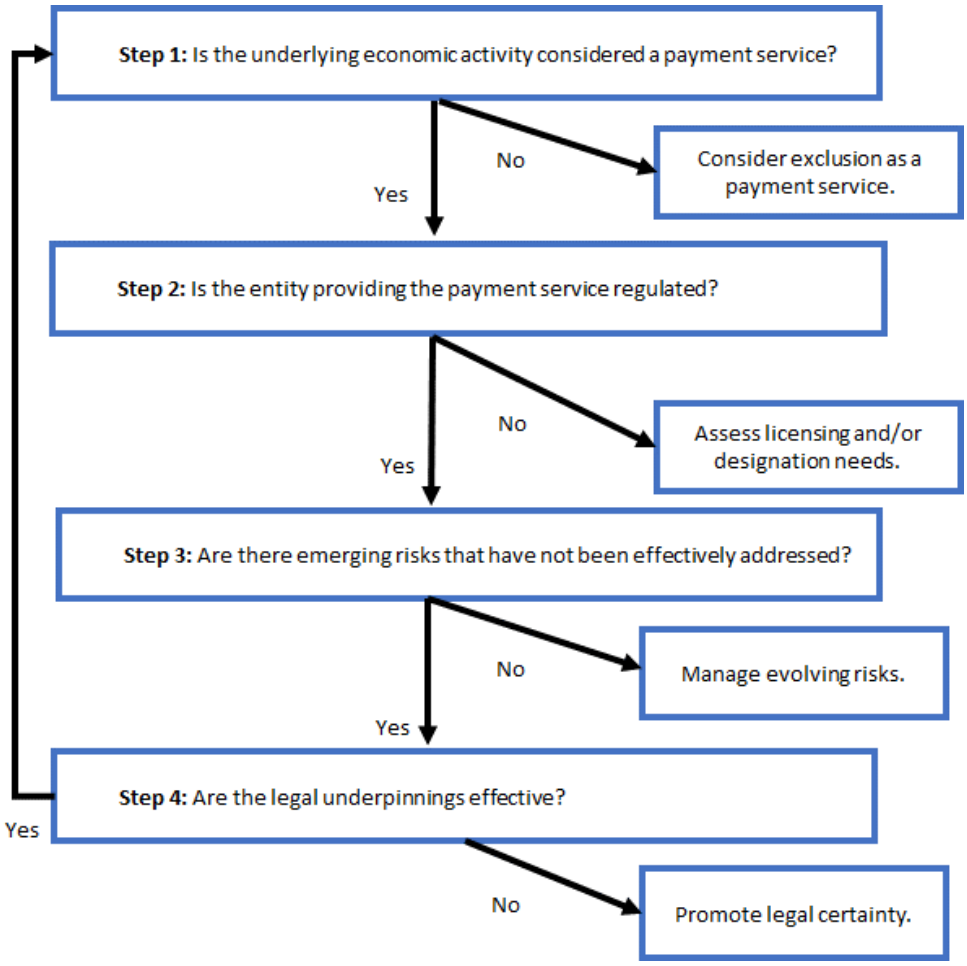
This paper proposes an analytical framework for regulating retail payment services and is aimed at strengthening their oversight and supervision. This is particularly relevant for countries whose retail payment oversight frameworks are evolving in response to the changing financial landscape. While there is currently a lack of international standards, there are emerging best practices.[3] Recent experiences are largely drawn from the European Union, Singapore, the United Kingdom and other relevant jurisdictions.[4]

The analytical framework is organized around four key steps (Figure 1). Although laid out in a sequential manner, certain steps in the framework may need to occur contemporaneously. That is, promoting legal certainty could be generally applicable throughout, and identifying and addressing regulatory gaps could be an exercise that is specifically sequenced. The remainder of the paper discusses each step. Section II identifies activities that are considered payment services. Section III discusses licensing and designation. Section IV examines the major risks and their management. Section V considers legal certainty. Section VI discusses policy issues for central banks. Section VII concludes.

[3] International principles and guidance of relevance have focused on systemically important payment systems (CPSS, 2001), oversight of payment and settlement systems (CPSS, 2005), national payment system development (CPSS, 2006), international remittance services (CPSS/World Bank, 2007), financial market infrastructures (CPMI/IOSCO, 2012), and payment aspects of financial inclusion (CPMI/World Bank, 2016).

[4] Nearly half of the regulatory agencies surveyed by the Basel Committee on Banking Supervision have considered new regulations or guidance related to Fintech (BCBS, 2018).

Figure 1. Analytical Framework for Payments Regulation



Source: Authors.

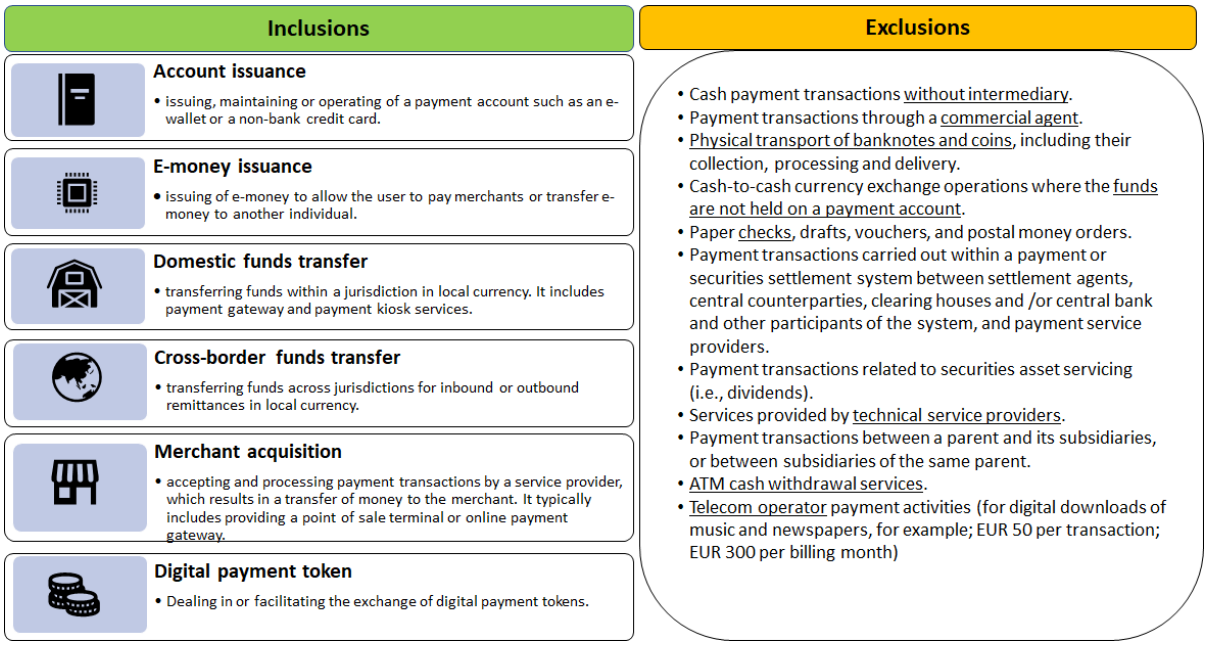
II. Step One—Identifying Activities as Payment Services

A. Payment Services

The first step of the framework is to identify if an economic activity undertaken by the entity is a payment service. Their identification helps to design effective oversight and supervisory frameworks, while avoiding unnecessary overlaps and/or duplication of regulatory efforts. International experiences suggest that such activities could be organized into 6 groups, including: (i) account issuance; (ii) electronic money issuance; (iii) domestic funds transfer; (iv) cross-border funds transfer; (v) merchant acquisition; and (vi) digital

payment tokens (Figure 2).[5] These mainly relate to services delivered to payment service users, and are not focused on payment systems.

Figure 2. Taxonomy of Payment Services



Source: Adapted from EU Payment Services Directive 2 and Singapore Payment Services Act. See full details in the legal instruments.

Explicit payment service laws help provide clarity on the activities. The EU Payment Services Directive 2 (PSD2) of 2015 (Article 4) provides a definition for payment services as any business activity associated with 8 types of activities annexed to the Directive.[6]

[5] This list is not exhaustive and could differ by jurisdiction. Some jurisdictions have introduced regulatory sandboxes, which is not in the scope of this paper. For illustration, see IMF (2019). Other new forms of payment services have included third party initiation, tokenization, payment gateways, payment aggregators, and white label ATM/POS providers, which are not in the scope of this paper. Digital payment token services are included based on recent market and regulatory developments.

[6] The EU PSD2 (Annex 1) groups payment services as: (i) services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account; (ii) services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account; (iii) execution of payment transactions, including transfers of funds on a payment account with the user's PSP or with another PSP; (iv) execution of payment transactions where the funds are covered by a credit line for a payment service user; (v) issuing of payment instruments and/or acquiring of payment transactions; (vi) money remittance; (vii) payment initiation services; and (viii) account information services.

Singapore's Payment Services Act (PS Act) of 2019 defines payment activities into 7 categories for the purpose of licensing (Part 2, Section 6; Part 1 of the First Schedule).[7]

Certain payment activities could be excluded from payment service laws. The EU PSD2 (Article 3) determines its non-applicability to 15 payment activities such as cash, paper-based payment instruments (checks, drafts, vouchers, postal money orders), and ATM cash withdrawal services in the EU.[8] The Singapore PS Act (Part 2, Section 13) exempts certain persons and entities from the requirement to have in force a license to carry on a business of providing any payment service, and describes clearly activities that are not considered payment services (Part 2 of the First Schedule) in Singapore.

Big Techs also handle payment services as part of e-commerce with some offering them as independent business units. Their business models leverage on their data analytics, network externalities, and interwoven activities, coupled with distinct platforms that process and settle payments, including: (i) *overlay system* (using third-party infrastructures such as credit card or retail payment systems); and/or (ii) *proprietary system* (using firm-owned infrastructures) (BIS, 2019). Some common business applications include digital wallets, online banking, and domestic and cross-border funds transfers. Table 1 provides an overview of payment services provided by selected Big Techs.

Table 1. Big Tech Payment Activities

	Approximate Offerings							
Payment Service	**Google Pay**	**Amazon Pay**	**Facebook Pay**	**Line Pay**	**Apple Pay**	**Baidu Wallet**	**Alipay**	**Tencent We Chat Pay**
Account issuance	Y	Y	Y	Y	Y	Y	Y	Y
E-money issuance	N	N	N	Y	Y	Y	Y	Y
Domestic funds transfer	N	Y	Y	Y	Y	Y	Y	Y
Cross-border funds transfer	N	N	N	N	N	Y	Y	Y
Merchant acquisition	N	Y	N	Y	Y	Y	Y	Y
Digital payment token	N	N	N	N	N	N	N	N

Note: For illustrative purposes and non-exhaustive. Other examples are in Africa (M-Pesa) and the Nordic countries (Swish, Vipps, MobilePay) among others. Some services are available in certain countries and not others. Based on publicly available information and not actual submission of business models.

Source: Authors.

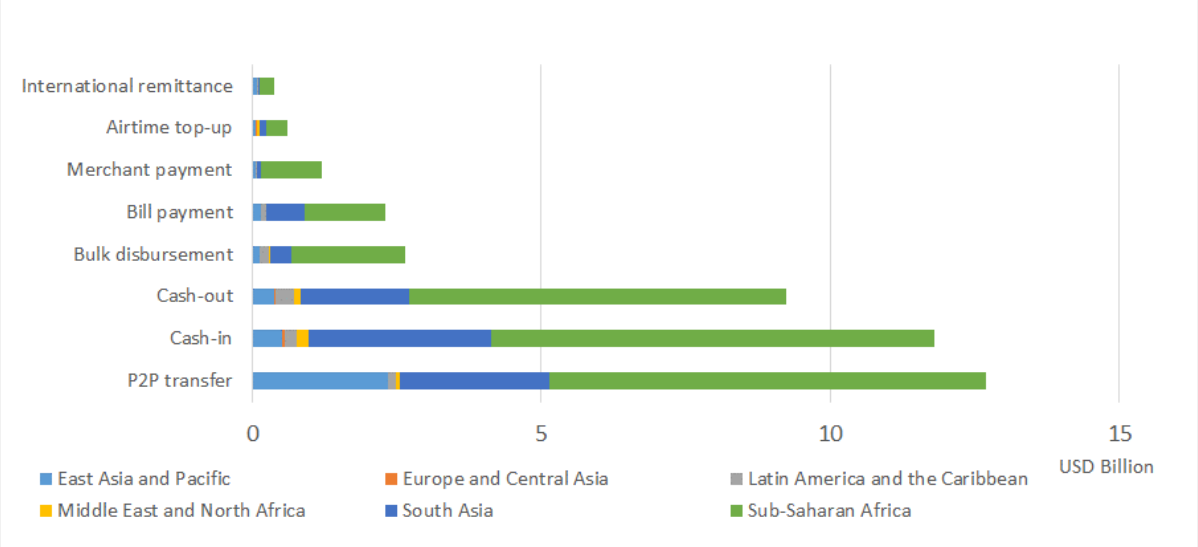
[7] This includes: (i) account issuance service; (ii) domestic money transfer service; (iii) cross-border money transfer service; (iv) merchant acquisition service; (v) electronic money issuance service; (vi) digital payment token service; and (vii) money-changing service.

[8] The identification or exclusion of certain payment services may vary across jurisdictions and does not imply that other relevant legislation or regulation are not applicable. For illustration, the penetration and use of mobile money may be more significant in some countries than others.

B. Mobile Money and Payments

Mobile money service delivery could be account-based or cash-based. Such services have distinct features from traditional banking, including: (i) transferring of money and making and receiving payments using the mobile phone; (ii) availability to the unbanked (people without access to a formal account at a financial institution); and (iii) exclusion of mobile banking or payment services that offer the mobile phone as just another channel to access a traditional banking product.[9] The high penetration of mobile phones has led to the proliferation of such services. Mobile money services offered by mobile network operators (MNOs) could be grouped into 8 payment-related activities for harmonizing statistical collection. [10] A large share of transaction values relating to mobile money services have originated from person-to-person transfers and cash-related activities as compared to air-time top-ups or international remittances (Figure 3).

Figure 3. Global Mobile Money Transaction Values by Activity and Region in 2018



Source: GSMA

[9] See Groupe Speciale Mobile Association (GSMA) Global Mobile Money program and dataset.

[10] This includes: (i) air-time top-ups funded from customer accounts (excluding purchases of airtime funded by OTC payments); (ii) bill payments using mobile money; (iii) bulk disbursement (such as salary payments, government or nongovernment organization transfers, regardless of whether they terminated in an account or OTC); (iv) cash-in to customer accounts (excluding OTC P2P payments, bill payment or airtime top-ups); (v) cash-out from customer accounts (excluding OTC collection of bulk payments or P2P payments); (vi) international remittance made between customer accounts; (vii) merchant payment, involving movements of value from a customer to a merchant to pay for goods or services at the point of sale using a mobile money account; and (viii) person-to-person transfers, including domestic transfers made between two customer accounts including OTC transactions, off-net/cross-net transfers, bank account-to-mobile account transfers, and mobile money-to-bank account transfers.

MNO mobile money services have posed regulatory challenges in many jurisdictions, given their growing systemic importance and light touch regulatory treatment. Risk-proportionate regulations have often been the approach taken in many jurisdictions, particularly for AML/CFT measures to prevent financial integrity risks. Such approaches facilitate financial inclusion and seek to avoid stifling innovation. But as their activities become more widespread with growth in customer base and transaction values, the potential financial stability risks could warrant monitoring by authorities. Supervisory vigilance is needed to ensure appropriate regulatory treatment, based on a substance-over-form approach, is applied to new products, particularly if these products become more complex, opaque, and blur the lines between different sectors. For example, MNO partnership with micro-finance firms to provide credit could also suggest that the underlying activity may not be solely a payment service and require separate regulatory treatment. Such ambiguous activities could reduce effective supervision and oversight. Indeed, in the case of telecom operators that were previously exempted from the EU PSD1, they now fall under the EU PSD2 following regulatory reforms with a few exclusions (Box 1).

Box 1. European Union—Payment Activities of Telecom Operators

Under the EU PSD1, payments made through a telecom operator were not covered, where the telecom operator acts as an intermediary between the consumer and the PSP (by operator billing or direct to phone-bill purchases).

Under the EU PSD2, the purchase of physical goods and services through a telecom operator now falls within the scope of the Directive. The exclusion for payments through telecom operators has also been further specified and narrowed down. The exclusion now covers only payments made through telecom operators for the purchase of digital services such as music and digital newspapers that are downloaded on a digital device or of electronic tickets or donations to charities.

To avoid the risk of exposure to substantial financial risks to payers, only payments under a certain threshold are excluded (EUR 50 per transaction; EUR 300 per billing month). Telecom operators that engage in such an activity shall notify to the competent authorities, on an annual basis, that they comply with these limits. The activity will also be listed in the public registers.

Source: European Commission.

C. Digital Payment Tokens

Digital payment tokens are a novel method using digital tokens for payments but remain largely untested. The emergence of stablecoins—crypto-assets whose value is linked to a pool of assets—have sought to address some limitations of earlier crypto-assets. Further, so-called global stablecoins (GSCs) have the potential to improve cross-border payment arrangements that have largely remained costly, slow, opaque, and fragmented.

Many regulatory concerns and risks relating to crypto-assets and potential GSCs would need to be addressed. While the underlying activity of crypto-assets could be associated to a means of payments or store of value, other features could resemble securities or

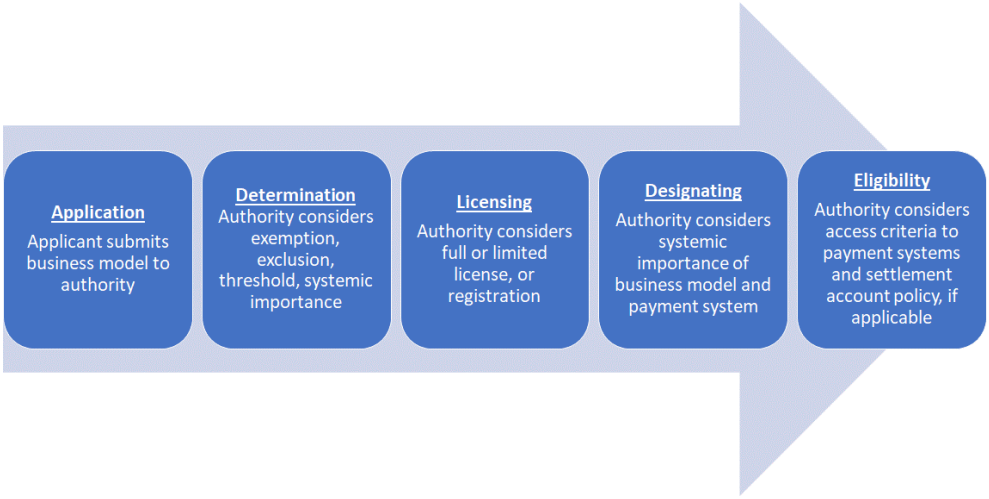
commodities. Regulatory gaps could arise if such assets fall outside the perimeter of market regulators and payment system oversight (FSB, 2019b; FSB, 2018). Potential GSCs have also raised challenges in multiple areas, including: legal certainty; governance and investment rules; financial integrity; safety, efficiency, integrity of payment systems; cyber security and operational resiliency; market integrity; data privacy, protection and portability; consumer/investor protection; and tax compliance (Group of Seven, 2019).

Digital payment tokens' benefits and risks need to be weighed against public policy goals. In the U.S., considerations were given to physical cash in circulation, reserve currency status of the US dollar, robustness of the banking system, and availability of digital payment options (Brainard, 2019). Broader implications include investor protection, consumer protection, data and privacy, systemic risk, monetary policy, and national security.[11] A few jurisdictions have initiated regulatory reforms to address digital payment tokens as a means of payment (Box 2).

III. Step Two—Licensing Entities and Designating Systems

The second step in the framework is to determine if an entity providing the payment service requires licensing or designation (if it is a payment system) (Figure 4)**.**

Figure 4. Licensing and Designation of Nonbank Payment Service Providers



Source: Authors

Regulatory responsibilities for payment-related activities are broad and have two distinct roles—prudential supervision and oversight. Supervisory and oversight powers are generally established in central bank laws and payment service laws. Prudential supervision targets PSPs. Oversight focuses on payment systems, critical service providers,

[11] United States House of Representatives Committee on Financial Services Hearing on "Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System", July 17, 2019.

payment instruments and schemes. These approaches are complementary. While oversight focuses on the sound and safe functioning of payment systems, payment instruments, payment schemes or other payment infrastructures, prudential supervision pursues safe, stable and secure financial institutions delivering payment services to users.

Box 2. Regulation of Digital Payment Tokens in Selected Jurisdictions

Singapore

The Singapore PS Act (Part 1, Section 2) defines digital payment tokens as: "any digital representation of value (other than an excluded digital representation of value) that (i) is expressed as a unit; (ii) is not denominated in any currency, and is not pegged by its issuer to any currency; (iii) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of debt; (iv) can be transferred, stored or traded electronically; and (v) satisfies such other characteristics as the authority may prescribe."

Switzerland

The Swiss Financial Market Supervisory Authority (FINMA) developed Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICO), which describe payment tokens (synonymous with cryptocurrencies) as: "tokens which are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer". The Guideline also describes utility tokens, asset tokens, and hybrid tokens (where asset and utility tokens are also classified as payment tokens, and in effect, are deemed to be both securities and means of payment). A Supplement further clarifies stable coin classifications and potential relevance of money laundering, securities trading, banking, fund management and financial infrastructure regulation.

United States

The New York State Department of Financial Services established a BitLicense for entities associated with virtual currency business activities. A bill (H.R. 2144 Token Taxonomy Act of 2019) was introduced to the U.S. House of Representatives (as of April 2019), which sought to define virtual currency as: "a digital representation of value that is used as a medium of exchange and is not currency".

Source: Monetary Authority of Singapore, Swiss Financial Market Supervisory Authority, New York State Department of Financial Services.

A. Licensing Entities for Prudential Supervision

Licensing processes typically start with the application process. Questions could arise with new business models. Payment service laws could exempt certain entities from licensing. [12] Further threshold values help determine their risk profiles, and hence, regulatory intensity. A criterion for access to regulated payment systems or payment schemes could also help address competition, innovation, and financial stability objectives. Licensing could vary with different criteria, such as capital requirements, fit and propriety, financial conditions,

[12] Singapore's PS Act (Part 2, Section 13) exempts specific PSPs from licensing, including licensed banks, merchant banks, finance companies, person licensed to issue credit cards or change cards, and any person or class of persons that may be prescribed.

incorporation, operational requirements, and public interest (Appendix 1 illustrates MNO licensing practices).

Entities offering payment services could be broadly grouped as banks and nonbanks. One approach to delineate these entities is to group them as: (i) credit institutions; (ii) electronic money institutions (ELMI); (iii) post office institutions; (iv) payment institutions (PI); and (v) national central banks.[13] Their identification helps determine the applicable laws, licensing and regulatory requirements, competent authority, and regulatory gaps.

Prudential supervision of payment institutions becomes more important if the institution collects client balances (e.g. in e-wallets). When services offered by PSPs are similar to deposit and current account services provided by banks (and effectively have the same fiduciary function), there is a clear role to play for prudential supervision to protect client balances.

PSP licensing differ across jurisdictions (Table 2)**.** Globally the licensing of payments and value transfer services are largely provided through other limited or varied financial licenses in addition to full banking licenses (BCBS, 2018). These licenses are usually issued for money service businesses or ELMIs (EMIs in the UK). Clearing and settlement services are offered through financial licenses outside the banking sector. A majority of jurisdictions were found to have no licensing category for services relating to the issuance and transfer of non-fiat digital currency. Licensing frameworks in some jurisdictions have responded to fintech-related changes.[14] Institutional contexts could also vary with regards to the competent authority, which could include the central bank (payments oversight department, foreign exchange department, or banking department) or other financial regulator.

Threshold values could help separate licensing and registration requirements (Box 3)**.** These could be set through benchmarking exercises for licensing and exemption purposes. Authorities would consider information such as the total amount of payment transactions in business plans as part of their benchmarking and consideration. The determination could be based on transactions over a period. For illustration, this could include average daily balances of e-money float, monthly averages of payment transactions in the preceding 12 months

[13] This classification partly draws on the EU PSD2.

[14] The ECB issued the Guide to Assessments of License Applications (second revised edition) in January 2019, which includes applications from fintech companies with an interest to becoming a credit institution. The Bank of England and Financial Conduct Authority established the New Bank Start-up Unit to consider applications from any firm seeking to be a bank. The Reserve Bank of India issued restricted payments bank licenses in 2015, which are subject to a minimum paid-up equity capital equivalent to USD 15 million. Account holders are restricted to a maximum balance of USD 1,500 and are issued with ATM and debit cards (with no credit cards).

Table 2. Licensing of Payment-Related Activities

Payment Service	Number of jurisdictions with available licensing category			
	Full Banking License	Limited Banking License	Other Financial License	No License
Providing payments and value transfer services	16	7	19	1
Issuance / transfer of non-fiat digital currency	6	2	7	12
Providing clearing and/or settlement of payment transactions or transactions in financial instruments	6	3	16	1

Note: The BCBS survey of licensing frameworks included agencies in 19 jurisdictions, including: Argentina, Belgium, Brazil, Canada, China, France, Germany, India, Italy, Japan, Luxembourg, Mexico, the Netherlands, Singapore, South Africa, Spain, Sweden, the United Kingdom and the United States. European regulators (the European Banking Authority, the European Commission and the ECB) are included.

Source: Adapted from BCBS (2018).

B. Designating Payment Systems for Oversight

PSP designation decisions could arise if they have high risk and systemic profiles. Authorities have had to weigh innovation against more regulations, that come with designation, such as with the growth of mobile money transaction values relative to other payment systems (Cooper et al., 2018) and potential GSCs that could create a global payment system serving a large segment of the world's population (Group of Seven 2019).

Systemically important payment systems (SIPS) are highly regulated given their potential to trigger or transmit systemic disruptions. This generally includes systems that are the sole payment system in a country or the principal system in terms of the aggregate value of payments; systems that mainly handle time-critical, high-value payments; and systems that settle payments used to effect settlement in other systemically important FMIs. Criteria that are often considered in determining the need for or degree of regulation, supervision, and oversight include: (i) the number and value of transactions processed; (ii) the number and type of participants; (iii) the markets served; (iv) the market share controlled; (v) the interconnectedness with other FMIs and other financial institutions; and (vi) the available alternatives to using the FMI at short notice. Authorities could also designate FMIs as systemically important based on other criteria that are relevant in their jurisdictions.

.Box 3. Licensing and Threshold Values in Selected Jurisdictions

European Union

PSPs could consider exemption from supervisory licenses if the monthly average of the preceding 12 months' total value of payment transactions, including any agent, does not exceed a limit set by the Member State but that, in any event, amounts to no more than EUR 3 million. ELMI licensing exemptions could also be considered if the total business activities generate an average outstanding e-money that does not exceed a limit set by the Member State but that, in any event, amounts to no more than EUR 5 million. Registration, in both cases, are required. Actual implementation could vary across jurisdictions such as waiver regimes to enable limited PIs/ELMIs to enter and compete in the market (National Bank of Belgium, 2019).

For illustration, the UK Payment Services Regulation establishes that a small payment institution (SPI) has an average turnover in payment transactions not exceeding EUR 3 million per month. Registration is cheaper and simpler than authorization, but SPIs are unable to provide payment services into other European Economic Area (EEA) member states. An authorized payment institution (API) has an average monthly turnover in payment transactions is over the EUR 3 million threshold and/or provides payment services in the European Economic Area (EEA). Electronic money institutions (EMIs) include: a small EMI (where the business does not generate more than EUR 5 million average outstanding e-money, and an authorized EMI (where the business will generate more than EUR 5 million average outstanding e-money.

Singapore

The Singapore PS Act establishes three types of licenses, including: (i) standard payment institution (SPI), (ii) major payment institution (MPI), and (iii) money changing. A threshold approach is adopted to distinguish SPIs and MPIs. SPIs are subject to lighter regulations than MPIs given their lower risk profile. Thresholds do not apply to money-changing licensees. The thresholds for SPIs and MPIs are as follows:

- An SPI licensee is allowed to have e-money float of up to SGD 5 million only (calculated as an average daily balance over a year); total transaction value of up to SGD 3 million per month only (averaged over 1 year) for any one activity; and total transaction value up to SGD 6 million per month (averaged over 1 year) for two or more activities.

- An MPI license is required if e-money float is above SGD 5 million (average daily balance over a year); total transaction value above SGD 3 million per month (averaged over 1 year) for any one activity; and total transaction value above SGD 6 million per month (averaged over 1 year) for two or more activities.

While a PSP needs only one license for one or any number or combination of activities, licensees need to obtain approval for any variation of license (e.g. to add a new activity to its business, the entity needs to obtain approval.

Source: EU Payment Services Directive, Second Electronic Money Directive, Payment Services Act of Singapore, UK Payment Services Regulation. The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011.

The risk profiles and regulatory intensity of payment infrastructures could help form designation decisions. For the purpose of this report, payment infrastructures comprise of payment systems, payment service providers, payment schemes, and critical service providers (Table 3), where regulatory intensity could differ as follows:

- **Highly regulated.** SIPS that handle large-value and time-critical payments are commonly subject to compliance requirements to national and international standards and are critical infrastructures.[15] CBRs are an activity subject to banking regulation, AML/CFT laws, and other relevant regulations. Non-SIPS are considered non-systemic, where a disruption could affect public confidence in payment systems or the financial system. Non-SIPS could be required to comply fully, or partly, with the relevant international standards for payment systems.[16]

- **Moderately regulated.** Proportionate regulation and threshold values have been commonly applied to promote innovation and competition in the payments market by PIs, ELMIs, MNOs, and money transfer operators (MTO). FMI critical service providers (CSPs), including information technology and messaging providers, are subject to oversight expectations from authorities.[17] Postal office institutions also provide postal payment services based on their own payment infrastructure and regulations.[18]

- **Less regulated:** Informal funds transfers (IFT) refer to money transfers that occur in the absence of, or are parallel to, formal banking sector channels.[19]

New payment infrastructures should be assessed on their risk profiles. Their key features could be associated with a SIPS or non-SIPS. Following identification, the application of the relevant international standards on FMIs, additional regulatory requirements that supplement payment regulations (banking law and regulations, securities law and regulations), and other relevant oversight and supervisory expectations could also be considered.

---

[15] Payment infrastructures identified as critical infrastructures could also be required to meet information security requirements and subject to regulation by the national cyber security agency.

[16] For illustration, the Monetary Authority of Singapore has a category for system-wide important payment systems. The Bank of Canada identifies non-SIPS as prominent payment systems. The ECB has categorized non-SIPs as (i) non-systemically important large-value payment systems; (ii) 'prominently important retail payment systems (PIRPS); and (iii) other retail payment systems (ORPS).

[17] See CPMI/IOSCO (2014).

[18] For illustration, the Universal Postal Union has established for member countries multilateral and licensing agreements, regulations, and service standards for its worldwide electronic postal payment network.

[19] See El Qorchi et al., (2003).

Table 3. Payment Infrastructures and Regulation

Risk	**High**		CSP	SIPS
	Medium		ELMI MNO PI	NON-SIPS CBR
	Low	IFT	MTO PPS	
		Low	**Medium**	**High**
		Regulation		

Note: Approximate regulatory intensity. Actual regulatory approach may differ.
Source: Authors.

IV. Step Three—Analyzing and Managing Risks

The third step in the framework is to identify any emerging risks that may not be effectively addressed in the current regulatory framework.

Risks could fall under 5 categories, including: funds protection, financial integrity, cyber/data security, access to payment systems, and interoperability (Table 4). The inherent risks for each payment service could differ depending on their nature of activity. For example, e-money issuance could pose high risk for the protection of customer funds and cyber/data security relative to interoperability issues.

Table 4. Risk Map—Rating Payment Activities by Their Potential Impact

	Approximate Risks				
Payment Service	**Funds protection**	**Financial Integrity**	**Cyber and Data Security**	**Access to Payment Systems**	**Interoperability**
Account issuance services	M	H	H	L	M
E-money issuance	H	L	H/M	M	L
Domestic funds transfer	H	H	H/M	H	L
Cross-border funds transfer	H	H	H/M	H	L
Merchant acquisition services	H	L	H/M	M	M
Digital payment token services	M	H	H/M	H	L

Note: Approximate inherent risks based on generic operating models. Actual risks may differ. H = High, M = Moderate, L = Low

Source: Authors

A. Funds Protection

To bolster user confidence in using electronic payment means, regulatory requirements are normally imposed to safeguard electronic money float and funds in transit. A need to carefully consider alternative mechanisms for fund isolation, safeguarding and protection is imperative as there are currently no international standards in this regard. Effective off- and on-site supervision is a pre-condition for any funds protection mechanism, and it is important to be apprised of their pros and cons.

Floats refer to the total amount of electronic money balance held by the issuer. Safeguarding measures help protect these funds against the risk of insufficient funds to meet customer demand for cash and insufficient assets to repay customers in event of a trustee's or bank's insolvency (GSMA, 2016). It is particularly important to note that even when a nonbank electronic money issuer places the customer funds in a segregated bank account, it only protects customers from the insolvency of that nonbank electronic money issuer itself, but the funds are still not protected from the insolvency of the bank appointed to safeguard the funds.

Funds in transit also need to be safeguarded. Funds in transit refer to funds received from a user by the payment entity for the provision of the goods or services but have not been paid out to the payee yet.[20] For payment activities relating to merchant acquisition and money transfer, funds in transit could be exposed to credit risk if the PSP holds on to customer funds at any point of the payment chain. While funds received by PSPs are required to be transferred to the beneficiary on a timely basis, it is common to have time lags of a few days before the funds are received by the beneficiary, especially where services are provided in remote areas of a country. The amounts collected and at risk can also be large in some cases, for example those funds collected by the postal service agent. To provide for more customer protection, authorities should subject the customer funds collected by these entities to the same safeguarding requirements as electronic money.

Pass through deposit insurance extends the protection of bank deposits in existing deposit insurance laws to funds in stored value facilities such as electronic money. This approach protects customer funds held in nontraditional access mechanisms. The approach has also been considered in other jurisdictions, particularly in Africa. However, pass through deposit insurance is subject to the definition of "deposits" in existing legislation and the fulfillment of conditions such as the establishment of custodial relationships, and the recording of identities and amount of funds of each actual owner. Such criteria help establish

[20] Funds in transit do not include those arising from payment and settlement processes such as in a check clearing system, which should be addressed by the payment system design.

a functional equivalence for similar services that may have deposit features and make them eligible for participation in the deposit insurance scheme.

Customer funds may also be covered by an insurance policy or some other comparable guarantee from an insurance company or a credit institution. [21] Such guarantees should not belong to the same group as the payment institution itself. The amount should be equivalent to that which would have been segregated in the absence of the insurance policy or other comparable guarantee. The amount should be payable in the event that the payment institution is unable to meet its financial obligations.

Central bank reserve requirements have been applied to address high concentration risks originating from major nonbank PSPs. Nonbank PSP have been required to hold such reserves to safeguard their customer funds, where use of mobile payments has been widespread. The People's Bank of China gradually introduced such measures to large technology firms that were active nonbank PIs (BIS, 2019). As of January 2019, such firms were required to hold 100 percent of customer balances in a non-interest-bearing reserve account at the central bank. This followed a series of measures introduced since January 2017 (where the nonbank payment institutions were required to hold 20 percent of customer funds in a single and segregated custodial account at a commercial bank) and January 2018 (where the ratio was raised to 50 percent subsequently).

B. Financial Integrity

Payment products and services have the potential of being used for money-laundering and terrorist financing. It is therefore important to impose anti-money laundering and terrorist financing (AML/CFT) regulatory requirements to maintain financial integrity of the payment transactions. The Financial Action Task Force (FATF) has developed the "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payments" to guide countries on how to apply a risk-based approach to implementing AML/CFT measures.[22] The report provides guidance on which entities could be considered the responsible parties of payment services, and subject to AML/CFT regulation. Countries do not have a lot of flexibility in designing AML/CFT controls as they have to adhere to the international standard. The risk-based guidances are intended to help countries mitigate risks posed by certain products or services by developing specific and targeted supervisory, regulatory, and/or enforcement measures.

FATF has also enhanced international guidance for regulating virtual assets (VA) and virtual asset service providers (VASP) to safeguard financial integrity.[23] The FATF uses the term virtual asset to refer to digital representations of value that can be digitally traded or

[21] The EU PSD2 (Article 10) includes safeguarding requirements.

[22] See FATF (2013).

[23] See FATF (2019).

transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value. That is, virtual assets are distinct from fiat currency, which is the money of a country that is designated as its legal tender. If a VA/VASP falls within the scope of a product, service, or activity that is covered by the FATF standard, it will be subject to AML/CFT requirements (subject to the CDD exemption for transactions below USD/EUR 1,000) even if representing a minimal risk in a particular jurisdiction at present. All VASPs must be subject to AML/CFT supervision, which should be commensurate with the nature, scale, and risks of their activities.

FATF requires countries to impose specified, activities-based AML/CFT requirements. The risk-based approach that is to be designed takes into account the nature, scale, and risks of certain activities. The EU, UK, and Singapore take a threshold approach to assessing the level of money-laundering and terrorist financing risk that PSPs' operations based on account balances and transaction volume, in deciding whether Know Your Customer (KYC) is required. For electronic money whose definition could be broad, the provision of certain electronic wallets (e-wallets) whose reach, use and capability are sufficiently limited or restricted, may pose lower money-laundering and terrorist financing risks and these countries may carve them out from regulations.[24] AML/CFT requirements have also been applied to reporting entities regardless of whether the transactions are in fiat currency or digital tokens in Singapore (IMF, 2019).

C. Cyber and Data Security

While new players and payment models promote innovation and competition, they also pose new cyber and data security risks.[25] This could be a major concern for open banking, where the payments account infrastructure of account servicing PSPs (largely banks) are made accessible to other nonbank PSPs (BCBS, 2019). While this helps create new payment services such as payment initiation and account information services by PIs and ELMIs, they could also raise risk levels if security requirements are not met by third-party nonbank PSPs.

Managing such risk is important not only as a safeguard against fraud and operational disruptions, but also for maintaining data privacy. From central banks' point of view,

[24] For illustration, the MAS has assessed that value stored on e-wallets with these characteristics carry low money laundering and terrorist financing risks and are limited in consumer reach, and therefore exempted from regulations based on the following: (i) it is used for payment or part payment of the purchase of goods from the issuer or use of services of the issuer, or both (such as a single entity shop issuing its own vouchers e.g. spas, restaurants, bookshops); (ii) it is used only within a limited network of franchisees or related companies; or (iii) all the monetary value stored in the e-wallet is issued by a public authority, or a public authority has undertaken to be fully liable for or provided a guarantee in respect of all the monetary value stored in the e-wallet, in the event of default by the issuer.

[25] For illustration, 7-Eleven Japan was reported to suspend its mobile payment application services after hackers compromised USD 500,000 from its customer accounts (July 2019). This prompted the company to compensate its customers and the Ministry of Economy, Trade, and Ministry to require the firm to strengthen its security.

safeguarding public confidence in payment services is of utmost importance. An increase in incidents could negatively affect public confidence and pose reputational risk to authorities for the lack of effective oversight. For example, the EU GDPR establishes the protection of natural persons with regards to the processing of personal data and on the free movement of such data to protect data privacy.

Banks and nonbank PSPs need to ensure that there are adequate risk management and implementation of controls to manage cyber risks. This is important in areas such as user authentication, data loss protection, and cyber-attack prevention and detection. In general, technology risk refers to risk of unsecured payment services and risk of service providers' weak IT governance. IT security focusing on measures such as antivirus protection, software updates and data backups is essential to mitigate the risk. Technology risk management principles could include: (i) establishing a sound and robust technology risk management framework; (ii) strengthening system security, reliability, resiliency, and recoverability; and (iii) deploying strong authentication to protect customer data, transactions and systems.

Efforts to enhance cyber and data security could make use of technical standards and guidelines, which form part of licensing requirements and regulatory compliance.[26] While international guidance to address cyber resiliency has been issued (CPMI/IOSCO, 2016), this has largely focused on their application to FMIs, which have greater systemic importance, and less so for PSPs. Nonetheless, several jurisdictions have developed specific national guidelines to address such concerns. Singapore has implemented cyber hygiene regulations and technology risk management guidelines that apply to all licensees that rely on technology to supply payment services. Under the EU PSD2, the European Commission has conferred mandates on the European Banking Authority, which includes security measures for electronic payments.

D. Access to Payment Systems

Access issues could arise with efforts to promote competition, innovation, and financial stability through the payment systems. This question is often raised with the entry of new players in the payments space, including the possibility from fintech firms and Big Techs. It is not entirely clear whether they should be given access, and if so, what are the inherent risks. Access to payment systems could help mitigate disruption risks, particularly from large technology firms that provide payment services to the wider public and settle bilaterally or through private settlement service providers. Generally, access is commonly restricted to financial institutions, which are required to meet high regulatory and supervisory standards

[26] For illustration, Belgian authorities require compliance by PIs and ELMIs of the following: (i) protection of sensitive payment data; (ii) strong customer authentication, common and secure communication standards; (iii) IT security policy; (iv) reporting of operational and security incidents; (v) collection of statistics on transactions, fraud and performance; (vi) business continuity arrangements; (vii) compliance with rule on card-based payment instruments; and (viii) compliance with payment account management rules (National Bank of Belgium, 2019).

and access criteria set by the payment system operator and central bank that acts as the settlement service provider.

Nonbank PSPs currently gain access to the payment system mainly through one of two channels although there are other variants. First, as a direct non-settling participant by connecting directly to a payment system to submit and receive payments but using another direct settling participant that holds a settlement account with the central bank. Second, as an indirect participant by sending payment instructions through a direct participant.

Access considerations may potentially be shaped by the public policy objectives of safety and efficiency. Broadening access could help improve the diversity of payment arrangements (particularly nonbank PSPs), reduce single points of failure, widen the type of transactions that can settle in central bank money (considered a safe and ultimate settlement asset that mitigates disruption risk from the failure of a private settlement service provider), and mitigate credit risks. Competition could also help create a more level playing field for nonbank PSPs and reduce reliance on settlement banks. Also, it could enhance efficiency and benefit consumers by improving transaction fees, transparency, and convenience. Risk-related participation requirements would need to be considered, ensuring operational, financial, and legal requirements are met by participants.

Access decisions could be based on setting specific eligibility criteria for:[27]

- **Authorized nonbank PSPs.** Eligibility is considered for major authorized ELMIs and PIs. This includes entities whose payment transactions have been determined to be at or above an established value threshold. That is, all ELMIs and PIs are not automatically eligible to gain direct access. They are only registered (without authorization).

- **Direct settlement participant.** Eligibility is considered by the payment system (or payment scheme),[28] the central bank (acting as the settlement service provider), and the competent supervisory authority (and financial intelligence unit, where appropriate).[29]

- **Settlement account.** Eligibility is considered at the sole discretion of the central bank, using supervisory assessment results from the competent supervisory authority. Nonbank

[27] For illustrative purposes, the eligibility criteria are drawn from recent experiences in UK (Bank of England, 2019; 2017). The first nonbank PSP joined a UK payment system on April 18, 2018. See press release.

[28] Common eligibility criteria include: participant status, settlement arrangements, legal documents, legal opinion, member/shareholder, costs, and compliance.

[29] Supervisory assessments include assess compliance with existing regulatory requirements for nonbank PSPs and focus on governance arrangements, safeguarding of customer funds, and financial crime. Nonbank PSPs that hold a settlement account at the central bank are also subject to ongoing supervisory oversight to ensure their compliance with regulatory requirements, including requirements to periodically commission independent audits covering key risk areas.

PSPs, however, are ineligible for reserve accounts (if their business models suggest no exposure to overnight liquidity risk) and intraday liquidity facilities.

E. Interoperability

Interoperability is often needed to reduce the risk of fragmentation in the payment services markets. With the wide range of payment services offered by a large number of entities, interoperability requirements have increased in recent years in many countries. For example, interoperability was one of the key components in the Single Euro Payments Area (SEPA)—a project that integrated the pan-European retail payment markets. In SEPA, the technical interoperability was achieved by standardization (ISO 20022, International Bank Account Number, SEPA Credit Transfer scheme, SEPA Direct Debit scheme) that aimed to prevent market fragmentation. Interoperability requirement could also be emphasized at the country level. The Singapore PS Act sought to reduce the risk of a fragmented payment ecosystem and enhance confidence in acceptance of e-payments. This gives the central bank formal powers to ensure interoperability of payment solutions, in the interests of consumers and market development.

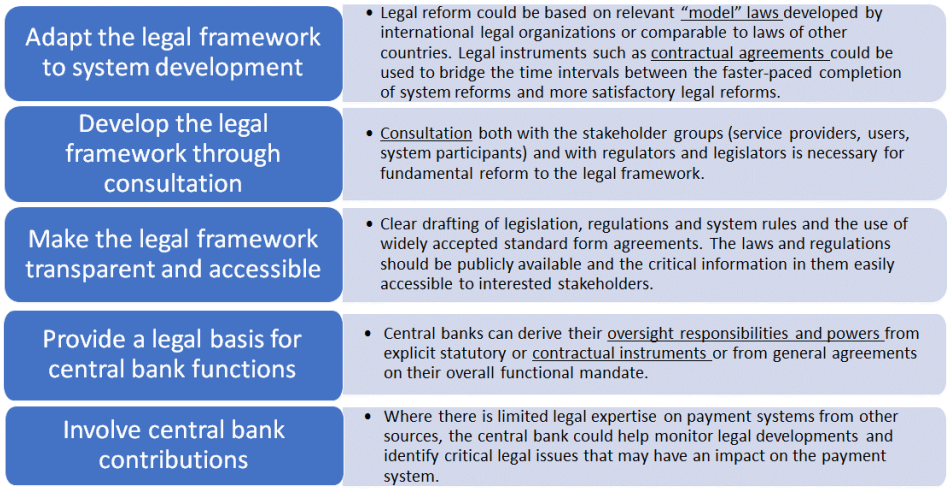
V. Step Four—Promoting Legal Certainty

The fourth step in the framework is to promote legal certainty through a transparent, comprehensive and sound legal framework for payment systems and services.

As payment services modernize, a sound legal basis is imperative. In response to the entry of large technology firms into banking, some authorities have followed the basic principle of "same activity, same regulation", where existing banking regulations have been extended to Big Techs (BIS, 2019). Questions on whether new technologies should adjust to law, or vice versa, could arise. If the former, the legal and regulatory frameworks for payments should be designed functionally (activity-based)—as opposed to an institutional approach—so that all providers of regulated services are regulated as per the general rules, and there is no need to adjust the legal and regulatory framework to technological innovation.

Promoting legal certainty is in fact a part of the general guidelines to develop national payment systems and are applicable to emerging payment services (CPSS, 2006). Some considerations include the legal framework, consultations, transparency and accessibility, and the role of the central bank (Figure 5; Box 4).

Figure 5. Key Considerations for Promoting Legal Certainty



Source: Committee on Payment and Settlement Systems (2006)

Box 4. Canada—Legal Reforms for Retail Payments Oversight

The Government of Canada has acknowledged that a range of new innovative service providers and technologies are emerging that are changing how Canadians make payments.

In Budget 2019, the Government proposed to introduce legislation to implement a new retail payments oversight framework, so that retail payment services providers could continue to offer innovation in services, while remaining reliable and safe. The framework would require payment service providers to establish sound operational risk management practices and to protect users' funds against losses.

The Bank of Canada would oversee the payment service providers' compliance with operational and financial requirements and maintain a public registry of regulated payment service providers.

The proposed legislative measure follows industry-wide consultations on a new retails payments oversight framework led by the Department of Finance Canada.

Budget 2019 also proposes to introduce technical amendments to the Canadian Payments Act to modernize the governance framework of Payments Canada. These proposed amendments follow a legislative review of the Canadian Payments Act undertaken by the Government in 2018.

Source: Department of Finance Canada (2019).

Although central bank oversight powers are largely drawn from their legal mandates, they may not be the plenary authority over payment systems, payment services, or other financial activities. The provision of digital payment token services, for example, could include the applicability of other laws and competent authorities (e.g. if tokens are identified as securities or financial instruments) or the need to develop new regulations or guidelines to provide greater legal clarity.

Authorities have adopted different approaches so far, including: regulating or increasing regulatory oversight for crypto-asset trading platforms, hosted wallets and certain

intermediaries; regulatory guidance, and consumer and investor warnings; registration or licensing; clarification of the legal status of crypto-assets for tax purposes; regulatory sandboxes for pilot testing under regulatory supervision; and bans on providing financial services to crypto-asset firms and/or on their use by financial institutions or for payment (FSB, 2018).

The legal framework for payment systems and services includes a body of law that determines the rights and obligations of parties in the system, including:[30]

- **Laws of general application.** Property and contract laws (creating legally enforceable rights and obligations to make and receive payments); banking and finance laws (establishing the rights and obligations of financial institutions to take deposits and make loans); insolvency laws (establishing the rights and obligations of creditors of an insolvent entity); laws determining which jurisdiction's laws apply (including contractual choice of law clauses and conflict of laws rules); and laws on electronic documents and signatures.

- **Laws specific to payments.** Payment instrument laws (currency laws, check laws, bill of exchange and electronic payment laws); payment obligation laws (netting, novation, finality of payment and settlement); laws on default proceedings and disputes in payments (priority ranking of payment settlement claims, settlement guarantees and loss allocation agreements, priority rights to collateral for settlement credit, evidence laws regarding electronic payments, and dispute resolution mechanisms such as arbitration clauses); laws on central bank roles, responsibilities and authority in the national payment system; and laws relating to the formation and conduct of infrastructure service providers and markets (formation and operation of clearing and settlement arrangements, access and participation in infrastructure systems, pricing of infrastructure services, rules on the issuance and redemption of e-money, and protection of central counterparties from risk).

Legal reforms could involve amending existing laws or regulations or introducing explicit law on payment services.[31] Benchmarking questions could arise as a result. As discussed, legal reforms could be based on relevant model laws developed by international legal organizations or jurisdictions.[32] Explicit laws on payment services has so far been

[30] The legal framework could be established by legislation or other statutory instruments, common law, administrative law, contracts (including system rules), or international treaties and regulations. The illustrations are not intended as a check list and depends on the institutional context in each jurisdiction.

[31] Swinehart (2018) suggests that payments regulation is largely technology-neutral and activity-based and is adaptable to financial change in the context of the U.S.

[32] For illustration, global electronic commerce and electronic payment activities have benefited from model laws developed by the United Nations Commission on International Trade Law (UNCITRAL), including: UNCITRAL Model Law on International Credit Transfers; UNCITRAL Model Law on Electronic Commerce (addressing issues of authorization, signature and evidence in electronic commercial transactions); UNCITRAL Model Law on Electronic Signatures; and UNCITRAL Model Law on Electronic Transferable Records

established in the EU PSD2 (and formerly the EU PSD) and the Singapore PS Act. For others, this could be more implicit and found in the legal framework for payment instruments, settlement of payment obligations, payment network organization and participation, or central bank oversight.

Laws on payment services interact with other core and complementary legislations. For example, while the EU PSD2 is one of the building blocks in the regulatory framework of the European services sector, there are other core legislations related to payment activities that are complemented with directives that address data protection, cyber security, and financial integrity (Box 5). Singapore is another jurisdiction that has introduced an explicit law on payment services, following efforts to streamline their existing regulatory framework.

Box 5. European Union—Key Legislations for Payment Related Activities

The basic building blocks for creating and supervising the single European market for payment services (excluding payment system regulations) include the following:

Core Legislations

- **Single Euro Payment Area (SEPA) Regulation.** This regulation establishes the technical and business requirements for credit transfers and direct debits in euro (introduction of the international bank account number and a domestic EU-wide payment area).
- **Payment Services Directive.** This directive (i) defines regulated payment services and the prudential supervisory regime applicable to its users and (ii) defines the rules on transparency for payment services and rights and obligations for payment service users and payment service providers.
- **Interchange Fee Regulation.** This regulation introduces the rules on the charging of interchange fees for card-based transactions.
- **Payment Account Directive.** This directive (i) establishes basic transparency requirements for fees charged by payment service providers, (ii) establishes the requirements for payment account switching procedures, and (iii) requires payment service providers to offer basic payment accounts.
- **Regulation (EU) 2019/518 of the European Parliament and of the Council of 19 March 2019 amending Regulation (EC) No 924/2009** as regards certain charges on cross-border payments in the Union and currency conversion charges.

Complementary Legislations

In addition, there are connected legislative acts applicable to payment services, including:

- **General Data Protection Regulation (GDPR).** This regulation establishes the protection of natural persons with regards to the processing of personal data and on the free movement of such data.

(allowing the use of transferable documents and instruments in electronic form). The EU Directive 98/26/EC on settlement finality in payment and securities settlement systems has also served as a useful benchmark.

- **Network and Information Systems Directive (NIS).** This directive provides legal measures to boost the overall level of cybersecurity in the EU.
- **Anti-Money Laundering Directive.** This directive strengthens EU rules to tackle money laundering, tax avoidance and terrorism financing.
- **Regulation (EU) No 1409/2013 of the European Central Bank of 28 November 2013 on payments statistics (ECB/2013/43).** Collects and compiles payment service statistics from all Payment Service Providers and statistics on participation and payments processed in payment systems.

VI. Policy Issues for Central Banks

Fintech developments in the payments space raises broader policy issues and challenges to the mandates of central banks, including:[33]

A. Payments Stability

Systemic importance. Large technology firms could have the potential to offer cross-border funds transfers through the issuance of digital payment tokens that would need to be assessed for their systemic implications and be required to meet the high regulatory standards, where appropriate.[34] Such service offering could, in effect, create a new payment system that could have a global outreach and operate independently from traditional CBR networks and financial messaging service providers. Authorities could face the challenge of licensing and designating the service offering as a SIPS, subjecting it to compliance with international standards, particularly the Principles for Financial Market Infrastructures (PFMI) (CPMI/IOSCO, 2012).[35]

Cross-border issues. Regulatory arbitrage could arise where a firm is registered as a crypto-exchange in one jurisdiction but as a payment service provider in another, raising similar issues to cross border banking regulation that calls for closer regulatory cooperation. Additionally, while some jurisdictions benefit from passporting rights, this could be unclear for others. Passporting rights could enable an entity (for example a PI/ELMI) to provide cross-border financial services from one jurisdiction to another without having a physical presence in the other country. Commitments for trade in financial services could differ across

[33] For illustration, Facebook's Libra initiative has such service offerings. Other broader public policy issues include competition, consumer/investor protection, tax compliance, which are beyond the scope of this paper.

[34] See Bank of England Warns Facebook Libra Faces Tough Scrutiny Before Launch, Financial Times, October 9, 2019.

[35] For illustration, the Swiss Financial Market Supervisory Authority has issued stable coin guidelines to clarify that such service offerings would require a payment system license and would be subject to FMI regulation and anti-money laundering laws. Additional requirements will also apply for bank-like risks in the payment system following the maxim of "same risks, same rules". Such requirements would relate to capital allocation (for credit, market and operational risks), risk concentration, and liquidity.

countries based on international, regional, and/or bilateral trade agreements. While some permit passporting rights for certain entities and activities, others could restrict them.[36]

Cooperative oversight. Central banks would also need to cooperate with other competent authorities (securities regulator, financial intelligence units) in considering additional regulatory requirements for other financial instruments or activities that are not considered payment activities to ensure the safety and security of payment and settlement arrangements. A key consideration could be determining the lead overseer and establishing regulatory cooperation among the relevant competent authorities for information sharing, cooperative oversight, and crisis management, as appropriate.

B. Financial Stability

- **Crypto-assets.** Regulatory gaps could arise when they fall outside the perimeter of market regulators and payment system oversight, and with the absence of international standards or recommendations (FSB, 2019a; FSB, 2019b; FSB, 2019c). Crypto-assets have been closely monitored for their potential financial stability risks at the international level (FSB, 2018).[37]

- **Big Tech.** Big Tech PSPs could have the potential to alter market structures and affect the degree of concentration and contestability. The unbundling of payment services (and other services) could put pressure on the profitability of traditional financial institutions and push them into riskier activities, posing financial stability concerns.[38] Big Tech PSPs could further leverage on their strong financial position, large customer base, name recognition, customer data, and global footprint to dominate the market. Such has been the case of China, where nonbank payment institutions have offered online money market funds and two firms have accounted for 94 percent of the mobile payments market (FSB, 2019a). Such high concentration risk could have destabilizing effect in the event of operational and cyber-related incidents.

- **Artificial intelligence (AI)/Machine Learning (ML).** AI/ML applications have rapidly evolved in financial services, including payments, and need close monitoring. Such technologies could be used to analyze large amounts of transactions data that help

[36] For illustration, the Nepal Rastra Bank was reported to have licensed a Chinese card company as a payment system operator to provide electronic card network and card clearing services (see article), and banned two Chinese payment institutions that were not registered but offering payment services to Chinese tourist visiting Nepal (see article).

[37] For illustration, the Monetary Authority of Singapore has monitored the digital token markets to analyze their material risks to financial stability (MAS, 2018). This includes the use of trading activity and net inflows in a fiat to digital token pair to proxy activity by a jurisdiction's participants.

[38] For illustration, the Monetary Authority of Singapore has conducted impact studies on the payments, deposit, and lending businesses of banks (MAS, 2017). For bank payment businesses, the studies used fee income from payment transaction volumes and fees data.

determine the usage patterns by customers, the creditworthiness of individuals and small businesses, and AML/CFT issues (FSB, 2017b). However, the use of personal data could raise issues relating to data privacy and data protections, particularly the separation of personal data from financial data. AI/ML also presents potential financial stability risks, including dependencies on third-party service providers, emergence of new systemically important players that fall beyond the scope of the regulatory perimeter, lack of interpretability or "auditability" of AI/ML methods, and opacity that may result in unintended consequences.

C. Monetary Stability

- **Mobile money.** Monetary policy transmission and central bank liquidity management could be complicated by the development of a payments system outside of the traditional banking system (such as with the widespread adoption of MNO mobile payments). Questions on the role and amount of float created from the issuance of e-money and/or mobile payments as an autonomous liquidity factor could also arise in jurisdictions where the use of such payment methods have become widespread. E-float could impact cash demand (an important element of autonomous funds forecasting), and also for free reserves held by the banking system (since they may be less certain when e-money floats would enter the banking system and impact individual banks). Such concerns were raised in the earlier issuance of e-money, where risk to monetary policy were later assessed as negligible given the limits placed on e-money accounts and the modest growth in transactions.[39] Similarly, virtual currencies were also assessed as having no significant implications for monetary policy. However, such assessments for mobile money and virtual currencies could change rapidly with their proliferation and evolving risks.

- **Digital payment tokens.** Potential GSCs could weaken monetary policy on domestic interest rates and credit conditions, increase cross-border capital mobility, and undermine monetary sovereignty if they substitute for fiat currencies (Group of Seven, 2019). The wide acceptance of crypto-assets, if materialized, could potentially reduce the demand for central bank money (He, 2018). That is, there could be a shift from account-based payment systems to token-based alternatives, with a focus on commodity money instead of credit money. Therefore, there is a role for central banks to make fiat currencies better and more stable units of account to maintain public trust in a digital, sharing and decentralized service economy. Many have initiated research into central bank digital currencies and experimented with distributed ledger technology in payment, clearing, and settlement arrangements.

[39] Studies have found that mobile money enabled effective monetary policy, transferring currency and assets into the formal financial system, enhancing their depth, and linked with a higher money multiplier (GSMA, 2019). Money supply was responsive to changes in the monetary base and improved the implementation of monetary targeting and the impact on the velocity of money and inflation were also unfounded in these studies.

VII. CONCLUSION

Fintech developments suggest that regulatory approaches and their legal foundations need to augment entity-based regulation with increasing focus on activities. Financial regulation has been traditionally based on the regulation of types of entities or intermediaries performing broad functions such as payment systems. Licensing regimes will need to be redesigned to bring new types of service providers within the regulatory perimeter where appropriate, including fintech firms and large technology firms.

A four-step analytical framework was proposed in this paper to guide authorities in regulating payment services. The first step examines if an underlying economic activity is considered a payment service. The second step determines if an entity requires licensing. The third step analyzes if there are new risks that have not been effectively addressed in the current regulatory framework, including risks associated with funds protection, financial integrity, cyber and data security, access to payment systems, and interoperability. The fourth and final step is aimed at promoting legal certainty to develop a transparent, comprehensive and sound legal framework for payment services.

Payments and fintech developments also pose policy considerations and challenges for central banks. Payment activities would need to be monitored for their growing systemic importance and impact on payments stability, financial stability, and monetary policy transmission. As payment activities evolve and potential systemic risks heighten, adherence to international standards and additional regulatory requirements would be warranted.

REFERENCES

Bank for International Settlements (2019). Big Tech in Finance: Opportunities and Risks, BIS Annual Economic Report 2019, June 23.

Bank of England (2017). Access to UK Payment Schemes for Nonbank Payment Service Providers, July.

Bank of England (2019). Bank of England Settlement Accounts, March.

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

Basel Committee on Banking Supervision (2019). Report on Open Banking and Application Programming Interfaces, November.

Brainard, L (2019). Digital Currencies, Stablecoins, and the Evolving Payments Landscape, Remarks at the Future of Money in the Digital Age, Washington, D.C., October 16.

Committee on Payments and Market Infrastructures (2014). Principles for Financial Market Infrastructures: Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers, Bank for International Settlements, December.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2012). Principles for Financial Market Infrastructures, Bank for International Settlements, April.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2016). Guidance on Cyber Resilience for Financial Market Infrastructures, Bank for International Settlements, June.

Committee on Payments and Market Infrastructures and World Bank (2016). Payment Aspects of Financial Inclusion, Bank for International Settlements, April.

Committee on Payment and Settlement Systems (2005). Central Bank Oversight of Payment and Settlement Systems, May.

Committee on Payment and Settlement Systems (2006). General Guidance for National Payment System Development, January.

Committee on Payment and Settlement Systems (2001). Core Principles for Systemically Important Payment Systems, January.

Committee on Payment and Settlement Systems and World Bank (2007). General Principles for International Remittance Services, January.

Cooper, B., C. Hougaard, L. Munoz Perez, C. Loots, R. Tuyeni Peter, M. Ferreira, and M. Dunn (2018). Payment Systems in Sub-Saharan Africa—Note 2: Case Studies of National

and Regional Payment Systems Market Development, Center for Financial Regulation and Inclusion, December.

Department of Finance Canada (2019) Investing in the Middle Class—Budget 2019, March.

El Qorchi, M., S. M. Maimbo., and J. F. Wilson (2003). Informal Funds Transfer Systems: An Analysis of the Informal Hawala System, Occasional Paper 222, International Monetary Fund, Washington, DC.

Financial Action Task Force (2013). Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, Paris, June.

Financial Action Task Force (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris, June.

Financial Stability Board (2017a). Financial Stability Implications from Fintech, June 27.

Financial Stability Board (2017b). Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications, November 1.

Financial Stability Board (2018). Crypto-Asset Markets: Potential Channels for Future Financial Stability Implications, October 10.

Financial Stability Board (2019a). FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications, February 14.

Financial Stability Board (2019b). Crypto-Assets: Work Underway, Regulatory Approaches and Potential Gaps, May 31.

Financial Stability Board (2019c). Regulatory Issues of Stablecoins, October 18.

Frost, J., L. Gambacorta, Y. Huang, H. S. Shin, and P. Zbinden (2019). BigTech and the Changing Structure of Financial Intermediation. BIS Working Papers No. 779, April.

Group of Seven (2019). Investigating the Impact of Global Stablecoins, October.

GSMA (2016). Safeguarding Mobile Money: How Providers and Regulators Can Ensure that Customer Funds are Protected, January.

GSMA (2019). The Impact of Mobile Money on Monetary and Financial Stability in Sub-Saharan Africa, March.

He, D (2018). Monetary Policy in the Digital Age, June, Finance and Development, Vol. 55, No. 2, pp. 13-16.

He, D., R. Leckow, V. Haksar, T. Mancini-Griffoli, N. Jenkinson, M. Kashima, T. Khiaonarong, C. Rochon, and H. Tourpe (2017). Fintech and Financial Services: Initial Considerations. IMF Staff Discussion Note 17/05, June, International Monetary Fund, Washington, DC.

International Monetary Fund (2017). Recent Trends in Correspondent Banking Relationships: Further Considerations. IMF Policy Paper, March, International Monetary Fund, Washington, DC.

International Monetary Fund (2019). Singapore Technical Note—Fintech: Implications for the Regulation and Supervision of the Financial Sector, July, International Monetary Fund, Washington, DC.

International Monetary Fund and World Bank (2018). The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech's Opportunities. IMF Policy Paper, October, International Monetary Fund, Washington, DC.

International Monetary Fund and World Bank (2019). Fintech: The Experience So Far. IMF Policy Paper, June, International Monetary Fund, Washington, DC.

Monetary Authority of Singapore (2017). Financial Stability Review, Macroprudential Surveillance Department, November.

Monetary Authority of Singapore (2018). Financial Stability Review, Macroprudential Surveillance Department, November.

National Bank of Belgium (2019). Financial Market Infrastructures and Payment Services, Report 2019.

Restoy, F. (2019). Regulating Fintech: What is Going On, And Where Are the Challenges? ASBA-BID-FELABAN XVI Banking Public-Private Sector Regional Policy Dialogue. Challenges and Opportunities in the New Financial Ecosystem. Washington DC, 16 October.

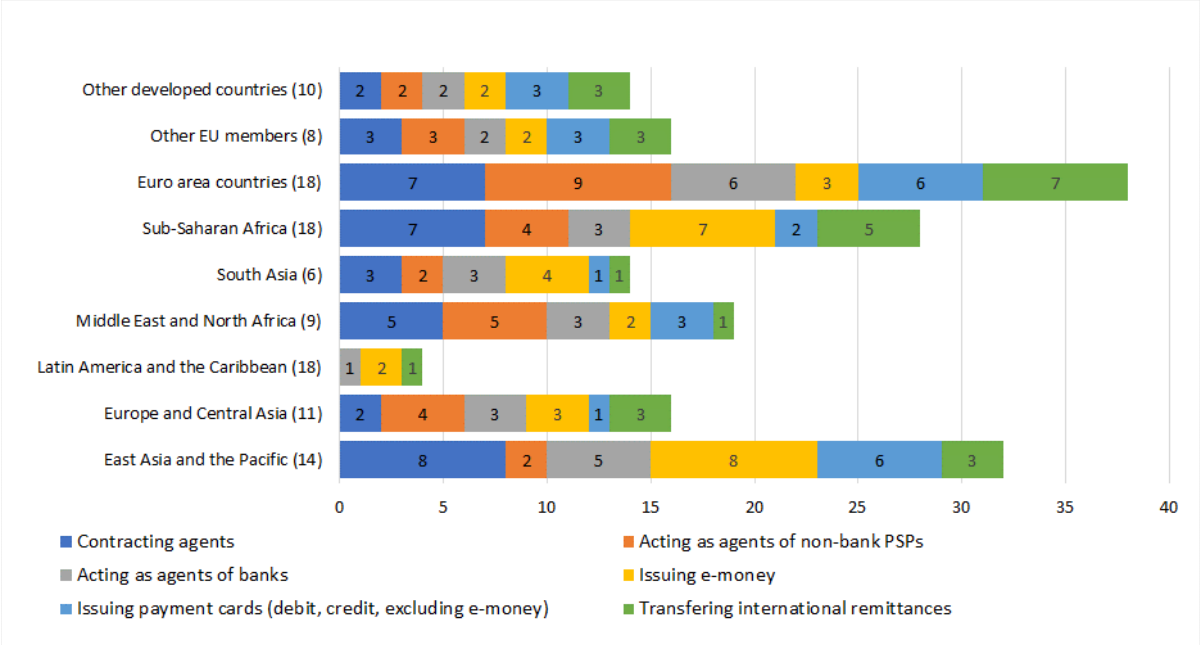
Swinehart, M. W. (2018). Modeling Payments Regulation and Financial Change, Kansas Law Review, Vol. 67(1), pp. 83-147.

Appendix I. Licensing Practices for Mobile Network Operators by Region

1. MNO Licensing

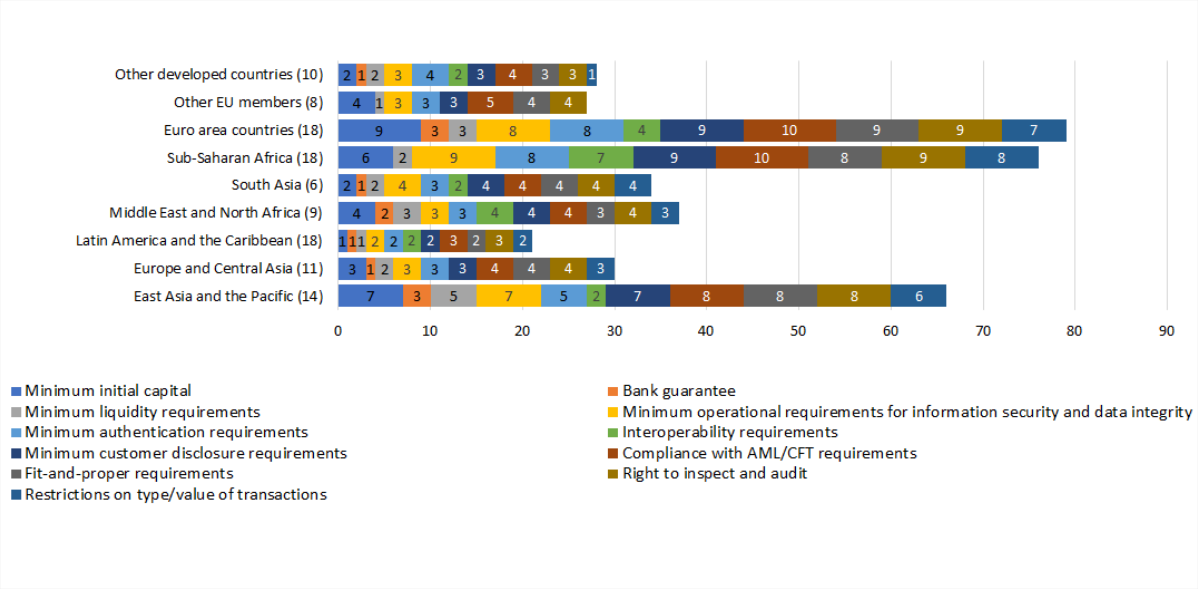
Source: World Bank (2018) Payment Systems Worldwide: A Snapshot, September.

2. MNO Admissible Activities



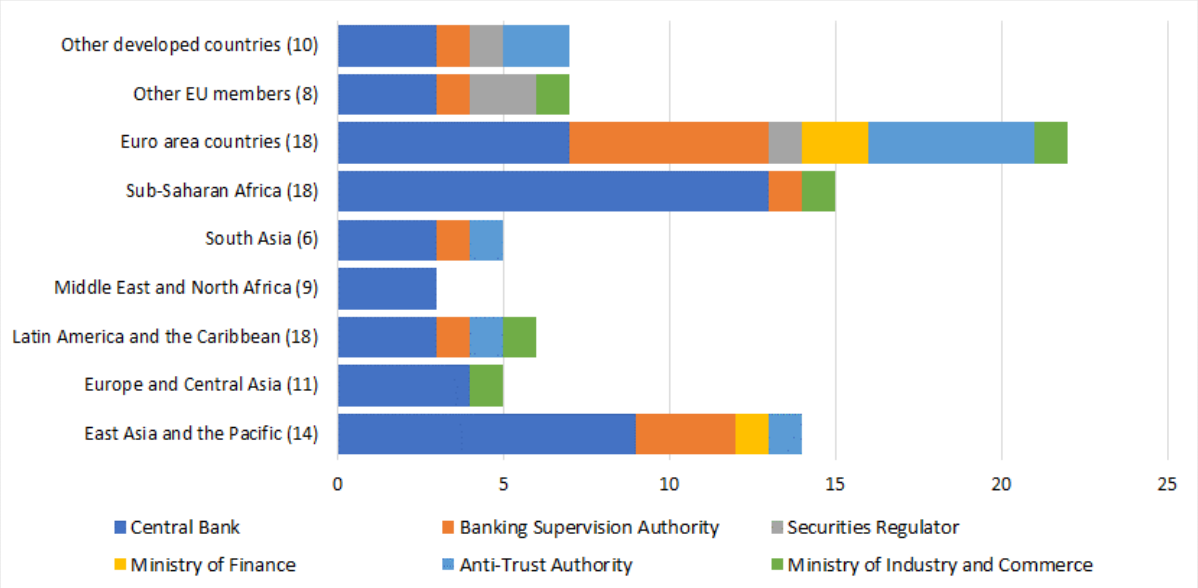
Source: World Bank (2018) Payment Systems Worldwide: A Snapshot, September.

3. MNO Licensing Requirements



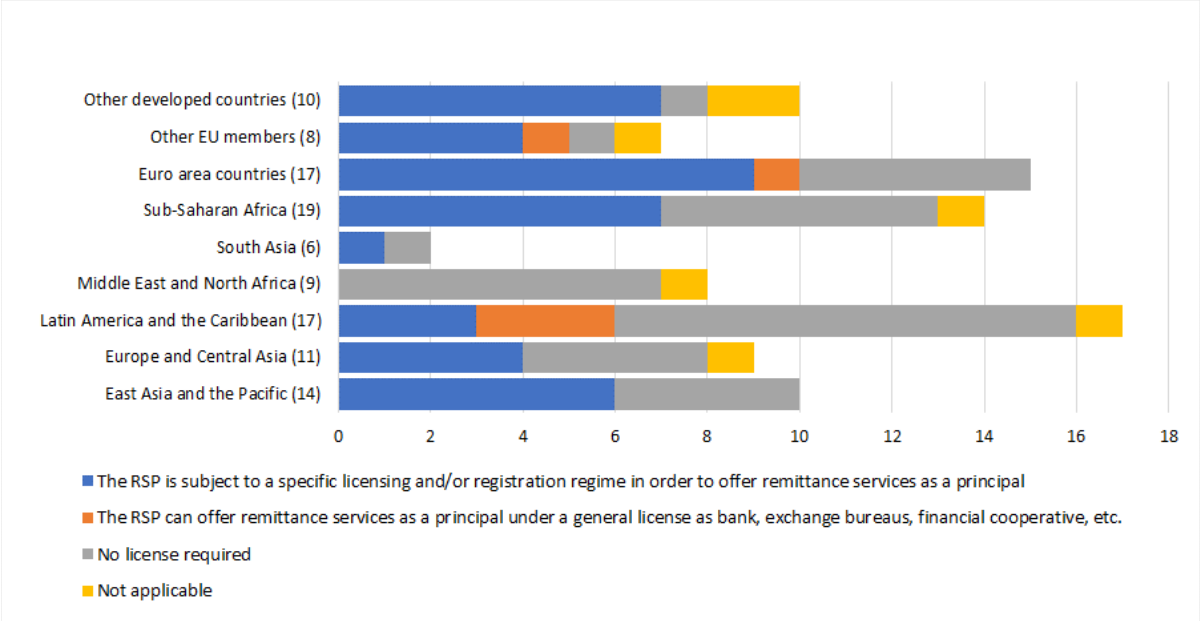
Source: World Bank (2018) Payment Systems Worldwide: A Snapshot, September.

4. Authorities Legally Empowered to Supervise MNOs



Source: World Bank (2018) Payment Systems Worldwide: A Snapshot, September.

5. MNO Licensing/Registration Requirements to Provide Remittance Services



Source: World Bank (2018) Payment Systems Worldwide: A Snapshot, September.