FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

Regulatory Aspects of Intermediaries in Electronic Payment Acceptance

ELECTRONIC PAYMENT ACCEPTANCE PACKAGE

WORLD BANK GROUP

ACKNOWLEDGMENTS
This report is a result of a collaborative effort across the World Bank Group's Finance, Competitiveness, and Innovation Department and the Financial Inclusion Global Initiative's Electronic Payment Acceptance (EPA) Working Group, which is funded by Bill and Melinda Gates Foundation.

This report was prepared by a team from the World Bank led by Ahmed Faragallah (EPA Innovations Workstream Chair, Senior Financial Sector Specialist) and including Daniel Salazar (Financial Sector Consultant) and Jeffrey Stephen Allen (Financial Sector Consultant).

Additional contributions were provided by Jose Antonio Garcia, Maria Chiara Malaguti, and Bernardo Barradas (World Bank consultants), who kindly reviewed this report, as well as by Charles Hagner, who edited the report. Naylor Design, Inc. provided design and graphics of the report.

The core team thanks Harish Natarajan (Lead Financial Sector Specialist) for his technical guidance and comments during development of the report and Mahesh Uttamchandani (Practice Manager) for providing the overall guidance to the working group.

Comprehensive EPA Innovations and Intermediaries Workstreams consultations were undertaken while preparing and reviewing the report. The workstream comprised Amina Tirana, Wameek Noor (Visa), Heba Shams (Mastercard), Ashley Olson Onyango (GSMA), Sohail Javaad (State Bank of Pakistan), Ma Haoyu (People's Bank of China), Mohamed Helmy and Mohamed Abdel-Rahman (Central Bank of Egypt), Elmuez Saber (Central Bank of United Arab Emirates), Jahongir Aminjanov (National Bank of Tajikistan), Gabriela Jaramillo Gabino (CNBV Mexico), and Vijay Chugh and Oya Pinar Ardic (World Bank Group).

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW, Washington, DC 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

DISCLAIMER
The Financial Inclusion Global Initiative led in partnership by the World Bank Group (WBG), International Telecommunication Union (ITU), and the Committee on Payments and Market Infrastructures (CPMI), with the support of Bill & Melinda Gates Foundation (BMGF). The FIGI program funds national implementations in three countries (China, Egypt, and Mexico), supporting topical working groups to tackle 3 sets of outstanding challenges in closing the global financial inclusion gap, and hosting 3 annual symposia to gather the engaged public on topics relevant to the grant and share intermediary learnings from its efforts.

This work has been prepared for the Financial Inclusion Global Initiative by the FIGI Electronic Payments Acceptance (EPA) Working Group. The work is a product of the staff of the World Bank with external contributions prepared for the Financial Inclusion Global Initiative. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including The World Bank, its Board of Executive Directors, or the governments they represent, or the views of the Committee for Payments and Market Infrastructure, International Telecommunications Union, or the Bill & Melinda Gates Foundation.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Table of Contents

Figures

Tables

Boxes

Acronyms

BNM	Bank Negara Malaysia
CBE	Central Bank of Egypt
CPMI	Committee on Payments and Market Infrastructures
EPA	electronic payment acceptance
EPAI	electronic payment acceptance intermediary
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FSB	Financial Stability Board
MSM	micro and small merchant
OCC	Office of the Comptroller of the Currency
POS	point of sale
PSD2	Revised Payment Services Directive
PSP	payment service provider
QR	quick response
RBI	Reserve Bank of India
SME	small and medium-sized enterprise
TPP	third-party processor

I. Introduction

1.1 THE FINANCIAL INCLUSION GLOBAL INITIATIVE AND ELECTRONIC PAYMENT ACCEPTANCE

The Financial Inclusion Global Initiative is a three-year program funded by the Bill and Melinda Gates Foundation in partnership with the World Bank, the Committee on Payments and Market Infrastructures (CPMI), and the International Telecommunications Union.[1] The Financial Inclusion Global Initiative established the Electronic Payment Acceptance (EPA) Working Group to foster effective practices for enabling and encouraging the acceptance and use of electronic payments, particularly among unserved and underserved segments. The EPA Working Group comprises national authorities, international financial institutions, donors, standard-setting bodies, and a wide range of private-sector stakeholders. It is premised on the concept that wide acceptance of noncash payments is a precondition for the uptake and effective usage of transaction accounts to perform most, if not all, payment needs, to store some value safely, and to serve as a gateway to other financial services.

The Financial Inclusion Global Initiative EPA Working Group, led by the World Bank, has developed a package of guides and technical notes (hereafter, "EPA package") that are intended to guide national authorities and stakeholders in the electronic-payment ecosystem while designing and implementing solutions and incentives to increase EPA. The EPA package comprises seven components: (1) EPA Package Reference Guide ("Reference Guide"), (2) Guidance for the Implementation of EPA Reforms ("EPA Reform Guidance"), (3) Self-Assessment Guide, (4) Incentives for Electronic Payment Acceptance ("Incentives Report"), (5) Innovations in Electronic Payment Acceptance ("Innovations Report"), (6) Regulatory Aspects of Intermediaries in Electronic Payment Acceptance ("Intermediaries Report"), and (7) Country Assessments. This note constitutes the sixth package component, the Regulatory Aspects of Intermediaries in Electronic Payment Acceptance.

Advancing the acceptance and usage of electronic payments globally is a critical economic-development imperative. As argued in the EPA package, electronic payments have important benefits for key economic stakeholders, including merchants, consumers, suppliers, payment service providers (PSPs), and governments. They also have clear benefits for the broader macroeconomy. Moreover, electronic payments have been crucial in facilitating economic activity during the ongoing COVID-19 pandemic. Despite the benefits of electronic payments, acceptance and usage have historically been sluggish in certain economies and economic sectors. The EPA package will assist national authorities and stakeholders in payment systems to advance the acceptance and usage of electronic payments.

The EPA Working Group is premised on the concept that giving individuals access to transaction accounts is a necessary, though not a sufficient, condition. Beyond achieving universal access—whereby all adults worldwide will be able to have access to a transaction account or an electronic instrument to store value and send and receive payments—there is also the key issue of whether a transaction account actually provides benefits to its users, which is very often reflected in how frequently that account is used, including to access other financial services. Wide acceptance of noncash payments is a precondition to the uptake and effective usage of transaction accounts to (i) perform most, if not all, payment needs, (ii) to store some value safely, and (iii) to serve as a gateway to other financial services.

Yet acceptance of electronic payments remains limited among merchants. It has been estimated that person-to-merchant payments to micro, small, and medium retailers (MSMRs) worldwide amount to $18.8 trillion, only 37 percent of which are made electronically (WBG 2016). Moreover, there is significant regional variation in EPA. Only 16 percent and 14 percent of MSMR payments are made electronically in Sub-Saharan Africa and South Asia, respectively. MSMRs tend to reuse cash received for the purchase of goods and services for supply-chain payments. Although 53 percent of MSMR business-to-business (B2B) payments globally are made electronically, the figure is propped up by high-income economies. The share of MSMR electronic business-to-business payments sits well below 53 percent in most regions. Thus, there is considerable scope for progress in expanding the acceptance and usage of electronic payments among MSMRs.

1.2 SCOPE OF THE REPORT

This report aims to foster effective legal and regulatory practices for enabling and encouraging EPA, one of the outstanding challenges for reaching universal financial access. It envisages a legal and regulatory framework that includes the regulation and licensing of *EPA intermediaries* (EPAIs)—that is, PSPs that support the acceptance of electronic payments in most cases by working with merchant acquirers. The report covers the following types of acceptance intermediaries: the merchants' facilitators or aggregators, third-party processors (TPPs), bill payment aggregators, and payment gateways. The report also provides an overview of the EPA ecosystem, the risks associated with EPAI services, and a deep dive into the approaches taken by different authorities to mitigate such risks.

A number of important dimensions to consider in regulating EPA activities are highlighted in the report. These include (i) the different types of risks associated with EPA activities; (ii) legal and regulatory policies to overcome such risks; (iii) samples of regulations in some countries/regions; and (iv) recommendations aiming to guide regulators, policy makers, and stakeholders in electronic-payment ecosystems when designing and implementing rules to discipline EPA while considering country context and national circumstances.

The report has been developed with an eye toward fostering the proportional and consistent application of regulation that is commensurate with the risks that are posed by underlying activities. Several important issues are addressed, including data protection, consumer protection, and funds protection. Finally, the report adopts a "technology-neutral" approach to regulation, which accommodates innovation and efficiency while preserving financial stability.

1.3 RELATION OF THE REPORT TO OTHER REPORTS AND WORKING GROUPS

The Financial Inclusion Global Initiative EPA package has been designed to assist EPA stakeholders with the first two phases identified in figure 1—self-assessment and the development of an EPA reform road map. While the EPA package can help inform implementation, it does not provide guidance on specific design and cost considerations, as these will depend heavily on local circumstances. The EPA package comprises the following seven components:

1. Electronic Payment Acceptance Reference Guide
2. Guidance for the Implementation of Electronic Payment Acceptance Reforms ("EPA Reform Guidance")
3. Self-Assessment Guide

FIGURE 1: EPA Reform Development Stages

4. Incentives for Electronic Payment Acceptance ("Incentives Report")
5. Innovations in Electronic Payment Acceptance ("Innovations Report")
6. Regulatory Aspects of Intermediaries in Electronic Payment Acceptance ("Intermediaries Report")
7. Country Assessments

Figure 2 captures the general relationships between the six package components beyond the Reference Guide. Ideally, EPA stakeholders should first consult the EPA Reform Guidance for a discussion of the wide range of programs and policies that can be pursued to enhance EPA, as well as a detailed overview of the Self-Assessment Guide and Incentives, Innovations, and Intermediaries reports. Second, stakeholders should leverage the Self-Assessment Guide to diagnose barriers to EPA in their local economy. The EPA Reform Guidance and Self-Assessment Guide are similar in that they are both guidance documents. Next, stakeholders can consult the Incentives, Innovations, and Intermediaries technical notes for more in-depth analysis of EPA-centric programs, policies, and innovations. Finally, the Country Assessments demonstrate how the EPA package components can be employed. The assessments combine elements of both self-assessment and road-map development. Wherever relevant, learnings from these assessments have been factored into the refinement of the EPA package components.

1.4 TARGET AUDIENCE

The intended audience for this report is primarily financial-sector regulators concerned with payment systems. The report also targets various stakeholders with an interest in expanding payment acceptance—namely, in understanding the approaches available to regulators to balance risks posed by the expansion and support for acceptance of micro and small enterprises to electronic payments through EPAIs. These stakeholders include, but are not limited to, banks and other financial institutions, and nonbank PSPs, including mobile-money operators and TPPs. Also included are fintech entrepreneurs who would like to deploy innovative services to improve solutions and value propositions supporting payment acceptance.

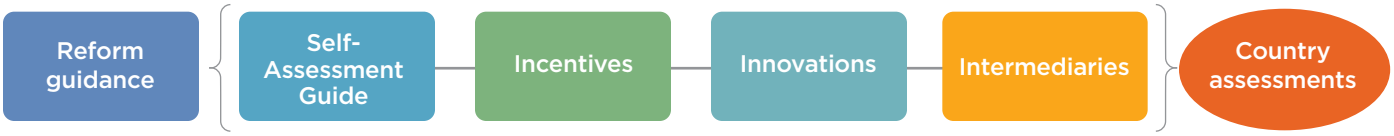
1.5 OVERVIEW OF CONTENT

This report focuses on regulating EPAIs. It is broken into five chapters. Following this introduction, chapter 2 sets the stage by introducing critical elements of payment systems, providing an overview of EPAIs, explaining the risks introduced by intermediaries, and establishing justifications provided by regulatory authorities for their regulation. The positioning of EPAIs within the payment-acceptance value chain is then highlighted. The chapter concludes by laying out—at a high level—three approaches for regulating EPAIs.

The next three chapters address these regulatory approaches in detail. Chapter 3 focuses on the direct regulation of intermediaries by authorities. Chapter 4 focuses on intermediaries as outsourcing providers to acquirers, describing necessary requirements for banks and nonbank acquirers. Chapter 5 describes an approach focusing on the payment scheme or payment system in which a scheme or system addresses intermediaries through its own rules. In addressing these three models, the paper focuses on several cross-cutting themes, including elements of regulation, licensing approaches, and relevant examples.

Different regulators possess unique resource endowments. Furthermore, each market has its own unique characteristics—institutions, resources, and level of market development. Given the unique characteristics and corresponding market structure of each market, it is important for regulators to understand the available options for addressing EPAIs within these different contexts.

FIGURE 2: EPA Package Component Relationships



2. Electronic Payment Acceptance Ecosystem

A successful payment system is characterized by a number of key components. Payment systems enable the exchange of value between payers and payees. Successful payment systems—characterized by high adoption and usage—possess several characteristics. They consist of many payers, who are in possession of a payment instrument, and a large number of beneficiaries, who are able to accept a payment instrument to conclude a transaction. This report focuses on the specific type of payments where payers are individuals acting as buyers and beneficiaries are businesses and, in specific, merchants, acting as sellers. A number of elements enable the transfer of value from the buyer to the seller. These elements include relevant products and services, corresponding business models, ecosystem participants, enabling infrastructure, and foundational rules and regulations.

Payment intermediaries have emerged to support and extend acceptance by micro and small merchants (MSMs), who, in turn, support the expansion of financial inclusion. Several questions arise regarding how best to balance the growth of inclusion with the mitigation of risks presented by intermediaries, and how these can best be managed. This chapter addresses questions stemming from the emergence of EPAIs. The first section provides detail on some of the key elements of payment systems. Section 2 focuses on acceptance intermediaries—many of which have emerged in the last decade—using definitions based on the functions they perform, to provide additional clarity. Section 3 focuses on the basis for the regulation of intermediaries. The chapter concludes with a discussion of three approaches to regulating intermediaries: direct, indirect through outsourcing arrangements, and through a payments scheme. Subsequent chapters will detail the three regulatory approaches.

2.1. KEY ELEMENTS OF A PAYMENT ECOSYSTEM

This section provides an overview of some of the critical features of a payment system and its supporting ecosystems. A payment system supports the transfer of value by defining how transfers are executed, providing a rules-based framework for users of the system, and often providing the technical infrastructure.

Payment acceptance is underpinned by an acceptance footprint. The ability to receive value for an electronic purchase is called payment acceptance. In payments—a two-sided market—payment acceptance is critical to the development and deepening of the system. Payment acceptance, however, has not generally received the same attention as *payment issuance* or the provision of pay-

ment instruments. Acceptance growth, to achieve a reasonable density and corresponding footprint, is necessary for a payment system to expand beyond providing access and the ability to make and receive transfers to enable the deepening of usage and improve the economics of the system. Payment acceptance occurs when businesses are willing to accept payment instruments for the purchase of goods and services and are provisioned to do so. Having highlighted the two sides of the market—issuance and acceptance—we now discuss and highlight developments on each side.

Instruments Enabling Electronic Payments by Payers

Electronic payments have advantages over cash payments. Electronic payments gained a lot of traction with the introduction of the plastic payment card. Payment cards have become ubiquitous in many parts of the world and synonymous with electronic payments. Like cash, they are tangible, enabling customers to make purchases. Unlike cash, they enable purchases to be made in non-face-to-face environments (for example, online), transcending distance. In some cases, they can be linked to additional accounts. Furthermore, electronic payment instruments provide consumers with protections against loss as well as some purchase protections through charge-back rights. What is unique is not the card, but the number on the card. The card is a form factor that enables the use of one's account number to facilitate the exchange of value.

New payment form factors have been introduced in the last three decades. Innovation has led to the introduction of new payment instruments, or form factors, to facilitate the electronic exchange of value. One is electronic money or e-money. Upon receipt of deposited funds or funds from a cash-in transaction, the e-money issuer will electronically credit monetary value to the instrument. E-money can be held on prepaid cards, devices such as mobile-money applications, or a server.

Another product is the electronic wallet, e-wallet, or digital wallet. An e-wallet is merely an application that acts as a container of other payment instruments, such as payment cards, bank accounts, or e-money accounts, and can be used online or at a merchant point of sale (POS). The e-wallet application provides access to the actual value stored at a card, bank account, or e-money account in the backend. The e-wallet is used because the mobile-phone applications can provide wide use cases to consumers and merchants and can be integrated seamlessly with different user or business applications.

Further forms of electronic payments exist, such as credit transfers and direct debits, where they are widely used in certain countries in certain use cases to purchase goods and services and pay bills.

Devices Enabling EPA by Payees

Technological innovation has driven improvements in acceptance devices. The traditional payment-acceptance device is a POS terminal. The terminal has evolved over the years, including changes to adjust to new types of communication and card types. For example, advances in communications have led to more connectivity options. Similarly, advances in chip technology have led to a migration in cardstock from magnetic stripe to chip cards. Further developments led to near field communications technology, where a transaction may be started by tapping a POS with the card. At present, after a dip or swipe of a card, POS devices can leverage an internet connection or dedicated phone lines to communicate with networks to transfer necessary payment information. Recently, the tokenization technology led to safer transactions over the internet by completely hiding the sensitive card information from transfer outside the well-fenced payment networks. The communication process facilitates the transfer of information, which results in the authorization of the transaction and enables its clearing and ultimate settlement.

Innovation has introduced lower-cost devices and means of acceptance. The mobile POS—also referred to as a dongle—is a lower-cost alternative to a traditional POS device. Its introduction was enabled by the emergence of smartphones, which provide for communication—in this case, network connectivity. The ability to leverage the communications capabilities of the smartphone has enabled the manufacture of lower-cost acceptance devices. Low-cost mobile POS have helped to fuel the emergence of a new payment-acceptance distribution model—enabled by payment facilitators—to expand acceptance footprints.

USSD had enabled the transfer of funds among persons and from persons to merchants using basic feature phones. The technology made a huge shift in the use of e-money in emerging economies, since it represented a low-cost option and was accessible by most of the mobiles, including non-smartphones. However, in some countries, USSD is monopolized by mobile-network operators or provided under discriminatory conditions and is unavailable as a service for financial institutions.

Another mode of acceptance enabled by smartphone technology is the quick response (QR) code. A QR code is a two-dimensional barcode comprised of black and white squares. The patterns formed by these squares can be read by smartphone cameras, POS terminals, or other devices to transmit the information necessary for a payment transaction. In the merchant-presented mode of QR code payments, merchants typically print a static

QR code that can be read by a phone to enable a transaction between the buyer and seller. This method requires negligible investment in acceptance infrastructure. Some merchants can present dynamic QR code generated from a mobile phone or any electronic device, where the transaction value and invoice number can be demonstrated within the code on each transaction. The merchant-presented mode enables push, as opposed to pull, payments. In the push model, which costs less and therefore is more relevant for our focus on MSMs, a buyer scans a merchant's QR code and initiates the payment from the buyer's end, often inputting the payment amount. The merchant then receives notification of the value credited to the merchant's account on the seller's phone, at which time the buyer can leave with the purchase. An alternative is the customer-presented mode, which generally requires more expensive acceptance infrastructure. In some cases, the customer-presented mode could be used to initiate a request-to-pay transaction. In this transaction, a merchant sends a payment-request message to the customer or payer. The payer is able to approve the request, initiating a credit-push transaction. The transaction is convenient for the customer, as all payment information is preentered by the merchant. It also provides benefits to the merchant in terms of speed of payments and visibility into the audit trail.

As will be further discussed in section 4, QR code providers often establish standards that govern payment transactions within their merchant networks.[2] These standards typically cover supported payment methods (for example, merchant-presented mode and customer-presented mode), authentication approaches, whether technical specifications are proprietary or harmonized, QR code types (for example, static or dynamic), and other key considerations (Nautiyal, Pors, and Martins 2020).

Card Schemes

Card payment is organized and managed by a card scheme. There are two types of card schemes for managing payments: a three-party and four-party model. The capabilities of a scheme are supported by a switch, which may or may not be part of the scheme. In addition to the elements already discussed, additional enabling elements include business models, corresponding infrastructure, ecosystem participants, and rules. The organization of a payment scheme and its key characteristics are described in chapter 5, which emphasizes those features relevant to payment acceptance.

Schemes manage the activities supporting electronic payments. A number of activities must be coordinated to enable electronic payments. These include branding, rules, licensing, and franchising, as well as, often, the operation and management of a payments switch. These roles and responsibilities can be collectively described as a payment scheme or, in the case of card-based payments through debit and credit cards, a card scheme. The standardization achieved by a scheme facilitates the processing of payments between participating parties in the payment ecosystem.

Switching enables the many-to-many relationships in electronic payments. A card switch—enabled in this case by scheme's network, rules, and technology—links members to provide three key services: authorization, which validates a transaction and funds availability; clearing, in which transaction details are transferred between relevant parties—issuers, acquirers, and, in some cases, the designated TPPs of acquirers—and settlement, in which the account associated with a transaction is credited to the acquirer, and the issuer is debited. A switch, in this case a card switch, is a routing center that transfers authorization requests, authorization approvals or denials, and transaction information to appropriate participants in the payment system. As a hub, it sits between numerous parities, facilitating one-to-one interactions between scheme members. A card scheme may possess its own card switch, which is the case of the international card schemes and most domestic schemes. In those cases where international schemes process payment information, they serve as the switch. There are numerous cases where domestic networks provide card switching for domestic schemes and sometimes for international schemes. This is the case in countries such as Mexico, where switching services are provided by two entities, Prosa and E-Global, each of which is owned by a consortium of banks. In other cases, the switch may be owned by a public authority

A scheme has more control in a three-party model. In a three-party model, a single entity maintains the relationship with both the cardholder and the merchant. Stated differently, the three-party model does not operate with intermediaries, such as issuers or acquirers. Under this structure, no fees or charges flow from an acquirer or issuer to the scheme operator. This model possesses a closed-loop structure, allowing the operator to capture more information about the payers than would be the case in a four-party model. This model is simpler and easier to coordinate, since the operator sets the rules and no intermediaries need to incorporate rule updates or changes into their operations. Because of the greater control it exercises over the value chain, the operator can act more quickly to make necessary changes than would be the case in a four-party model.

Examples of payment brands using this scheme structure are Discover Card, American Express, and, before it was bought, Diners Card. More recently, schemes operat-

ing under a three-party model have partnered with issuers to increase the number of their cards in circulation, but this has not changed the underlying model. The issuer owns the customer relationship, but a branded scheme will accept transactions through its acceptance footprint and process the transactions. Mobile-money schemes tend to apply the three-party model; they acquire the e-money account holders and merchants directly. Some mobile-network operators acquire merchants through intermediaries, while others prefer direct contracts with the merchants.

It is easier to build a larger acceptance footprint through a four-party model. A transaction processed over a network using a four-party model—beyond the payment scheme operating the model—involves four parties: a cardholder, a merchant, an issuer or the cardholder bank, and the acquirer, also called the merchant's bank. The four-party model is distinct from the three-party model in separating the role of issuer and acquirer. The scheme operator establishes the rules for operating the system. In many cases, the scheme also acts as a switch, routing transactions between issuers and acquirers.

One advantage of the four-party model is that it scales more easily than the three-party model. Schemes enlist others to develop their payment-acceptance footprint. This makes it easier for a four-party scheme to drive the network effects that are critical, especially in emerging economies, as well as extend their reach to excluded population segments. As entities or service providers join a four-party scheme, their end customers are accessible to other entities participating in the system or model. Schemes are open to any bank and, under certain conditions, to non-bank financial institutions that wish to participate as long as they comply with the rules of the scheme. For this reason, the model is often referred to as an open-loop system. As opposed to the closed-loop nature of the three-party model, it is more difficult to capture customer data, because of the model's more distributed nature. The four-party model is deployed by well-known payment brands, including Visa, Mastercard, China Union Pay, JCB International, and a large number of domestic schemes.

Mobile-Money Schemes

Common practices are emerging in mobile money. The use of mobile money for EPA has become common, especially in Sub-Saharan Africa. Many mobile-money service providers offer merchant-specific services and are working to build merchant networks (Katakam 2014). A GSMA survey of a central African economy found that merchants use mobile money extensively for customer payment acceptance and paying bills (Pasti and Nautiyal 2019). Though there are no industry standards akin to the payment card market, some observers, especially GSMA, have documented common practices among these merchant-centric services. Mobile-money schemes depend heavily on agent networks to reach out to their customers.

Four functions define emerging mobile-money schemes. With the introduction of mobile payment, we have seen the emergence of mobile-money schemes to organize the activities associated with this new type of payment. A potential working definition of mobile-money scheme is the following: A mobile-money scheme, which is governed by a mobile-money service provider, sets out operational arrangements for payments among its different segments of customers, including merchants. The scheme rules lay out the obligations of the provider, merchants, and consumers. Mobile-money scheme rules often cover the settlement process, dispute resolution, customer support, training, and, occasionally, other relevant issues, such as reversals.

Merchant Acquirers

Merchant acquirers are an essential part of the payment life cycle, as they provide payment services to merchants. Definitions of acquirers are extensive. Table 1 captures a group of relevant definitions. Acquirers are integral to Visa's and Mastercard's scheme rules. They provide high-level definitions of acquirers that are better understood within the context of the rules as a whole. The World Bank Group and the Committee on Payment and Settlement Systems (CPSS), the precursor to the CPMI, provide more conventional definitions of acquirers. The European Union, meanwhile, takes a functional approach to defining the "acquiring of payment transactions" (EU 2015a, article 4[44]).[3] This approach is meant to avoid excluding certain types of untraditional entities that engage in acquiring services.

What is clear from these definitions is that a merchant's ability to accept electronic payments runs directly or indirectly through an acquirer.[4] A merchant can deal directly with an acquirer or indirectly through an intermediary acting on behalf of an acquirer, when permissible. Importantly, merchant acquirers can be bank or non-bank entities. Additionally, merchant acquiring is not unique to card-based transactions. Payment acceptance via other form factors, such as mobile money and QR code–based payments, also involves merchant acquirers.

Clearing and settlement are central functions of merchant acquirers, but they often engage in an extensive range of other functions. To foreshadow a bit, section 2.2.1 lays out in detail the functions that can be performed by acquirers and payment facilitators, an important type of acceptance intermediary. Later, table 2 (see section 2.2.1) groups these functions into four broad categories.

TABLE 1: Common Definitions of Merchant Acquirers

Entity	Definition
Visa	"A Member that signs a Merchant or Payment Facilitator agreement, provides a Cash Disbursement to a Cardholder, or loads funds to a Prepaid Card, and directly or indirectly enters a Transaction into Interchange" (Visa 2020, 798).
Mastercard	"A Customer in its capacity as an acquirer of a Transaction" (Mastercard 2020, 367).
World Bank Group	"The entity or entities that provide services to the card acceptors (merchants) related to clearing and settlement of the accepted transactions. In general, the services include receiving and processing the data relating to the transaction for authorization, clearing and settlement, though some only provide services for clearing and settlement. Some acquirers also hold deposit accounts for card acceptors (merchants)" (WBG 2012, 86).
CPMI (formerly CPSS)	"The entity or entities that hold(s) deposit accounts for card acceptors (merchants) and to which the card acceptor transmits the data relating to the transaction. The acquirer is responsible for the collection of transaction information and settlement with the acceptors" (CPSS 2003, 7).
European Union	"'Acquiring of payment transactions' means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee" (EU 2015a, article 4[44]).

In the absence of an acceptance intermediary, such as a payment facilitator, acquirers typically engage in all such functions, in addition to maintaining the relationship with the underlying scheme. Indeed, an acquirer always maintains the relationship with the scheme. If an acceptance intermediary plays a role, the acquirer bears responsibility for the activities of the intermediary.

Mobile-Money Interoperability

Interoperability drives network effects and improved system economics. Interoperability is critical for maximizing the utility of payments for consumers and merchants, especially small merchants. More specifically, interoperability enables the development of network effects. Network effects derive from the large-scale use of a payment system, characterized by robust issuance and acceptance of payment products. This, in turn, drives greater utility and value for system participants. Furthermore, the usage stemming from interoperability and the network effects it drives improves system economics for operators and participating intermediaries.

In the mobile paradigm, the focus of interoperability is across schemes and channels. GSMA defines mobile-money account-to-account interoperability in two ways: (1) the ability of customers to make transfers between accounts held with different mobile-money schemes, and (2) transfers between a mobile-money account and an account at a bank. The concept of interoperability in mobile money is constructed differently than in the case of card interoperability—in which network effects stem from additional branded cards and the expansion of the associated branded acceptance footprint. While defined differently between cards and mobile money, interoperability in both cases is concerned with associated network effects. GSMA's definition of interoperability in mobile money is broader because a mobile-money account could be interoperable with another mobile-money account or bank account, regardless of scheme as in the case of cards or bank. Furthermore, interoperability with a bank account assures fund access across a number of channels and their associated touchpoints. On the other side, mobile-money interoperability is not fulfilled among different service providers in many jurisdictions, and trials for global interoperability among mobile-money service providers are very shy, contrary to cards interoperability.

There are additional dimensions to mobile interoperability. While not addressed by GSMA, there is a question of interoperability at the agent level, or agent sharing. Agents sharing is the case where an agent is not exclusively bound to one mobile scheme, but is instead able to support the services of a number of schemes—mainly, cash in and cash out, while keeping different liquidity pools. For example, the Regulatory Framework for Mobile Payment Systems in Nigeria of 2009 provides that agents are not restricted to any one scheme operator and can serve as agents to multiple operators. This is slightly different than POS terminal interoperability in card payments, where the same acquirer supports the ability of a POS terminal to accept multiple payment marks through a single device in a classic four-party model but using a single pool of liquidity.

2.2. ACCEPTANCE INTERMEDIARIES

The following sections outline definitions and functions of the following acceptance intermediaries: payment (merchant) facilitator, payment (merchant) aggregator, third-party payment processor, payment gateway (for online transactions), and bill payment aggregator.

Payment (Merchant) Facilitator

Explicit discussions of payment facilitators are found in Visa's and Mastercard's rulebooks. Visa defines a payment facilitator as a "Third Party Agent or non-Member VisaNet Processor that deposits Transactions, receives settlement from or contracts with an Acquirer on behalf of a Sponsored Merchant."[5] Mastercard defines a payment facilitator as a "Service Provider registered by an Acquirer to facilitate the acquiring of Transactions by the Acquirer from Submerchants."[6] In general, the Visa and Mastercard definitions appear to be very similar.[7]

Card scheme rules typically stipulate that payment facilitators are the only acceptance intermediaries that are allowed to access funds for the purpose of paying submerchants for card-based transactions. (See, for example, Mastercard 2019, section 7.3, page 146.)[8] Additionally, scheme rules often require submerchants to open a merchant account directly with an acquirer when they eclipse specified revenue thresholds—$100,000 for Visa (Visa 2020, 328) and $1,000,000 for Mastercard (Mastercard 2019, section 7.6.5, 149; Mastercard 2020, section 7.8, 160). Thus, payment facilitators are generally geared toward MSMs. Indeed, they play a pivotal role in extending EPA capabilities to MSMs globally (Miller and Salazar 2013; Govil 2016; WBG and WEF 2016).

Select central banks define payment facilitators similar to Visa and Mastercard. For example, the Reserve Bank of Australia defines a payment facilitator as "an entity which arranges or procures acquiring services from an acquirer for one or more merchants" (RBA 2016, section 2.3, 4). The Central Bank of Egypt (CBE) defines a payment facilitator as an entity that "provides financial and technical services through alternative delivery channels of its submerchants with which contracts have been concluded on behalf of the bank for the provision of e-Payment services" (CBE 2019, 6).

The key functions of a payment facilitator are summarized in table 2 and organized into four broad functional areas, which include (i) merchant onboarding, (ii) payment processing, (iii) ongoing security, and (iv) administrative and relationship management. Clearly, payment facilitators perform a broad range of functions across the acceptance value chain.

To summarize, a payment facilitator is an intermediary that onboards and processes payments for merchants through its own banking relationship and merchant identification number. What distinguishes a payment facilitator from other intermediaries involved in payment processing is that it is directly involved in settlement and it often frees a merchant from having to open a merchant account with a traditional acquirer. As such, a merchant that has an account with a payment facilitator, rather than an acquirer, is classified as a submerchant of the payment facilitator. The payment facilitator, in turn, processes payments on behalf of many submerchants through a single bank account.

TABLE 2: Payment Facilitator Functions[9]

Functional Area	Function
Merchant onboarding	Take applications and sign up merchants Set up technical mechanism for accepting transactions Customer due diligence Market development
Payment processing	Route authorization requests Clearing-file preparation Settlement Pay submerchants
Ongoing security	Ensure PCI-DSS compliance Monitor merchant activity Deter fraud
Administrative and relationship management	Transaction reporting to merchants and acquirers Customer service Risk management Education and training Value-added services

Payment (Merchant) Aggregator

Visa and Mastercard do not discuss aggregators in their rulebooks. The most explicit definitions of payment aggregators come from the Reserve Bank of India (RBI), the CPMI, the US Chamber of Commerce, and an e-commerce note from the World Bank Group. Table 3 catalogs definitions from these entities. The CBE also defines "Technical Payment Aggregators," which are discussed further below.

The clear emphasis in these definitions is that payment aggregators absolve small merchants of the need to open a merchant account with an acquirer. As the name implies, they *aggregate* merchant payments for processing through their own account. From the definitions contained in table 3, ***it is not clear that there is any difference between aggregators and facilitators.***

The CBE takes a different approach. It draws a fairly clear distinction between payment facilitators and "Technical Payment Aggregators" in Egypt (CBE 2019). The CBE defines the latter as an entity "that provides technical services to its sub-merchants on behalf of the bank through alternative delivery channels of the technical payment

TABLE 3: Definitions of Payment Aggregator

Entity	Definition
Reserve Bank of India	"Service providers who process the payment transactions of e-commerce merchants. Aggregators allow merchants to accept card and bank transfers without having to set up a merchant account with a bank or card association" (RBI 2019a, 18).
	"Entities that facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own. PAs facilitate merchants to connect with acquirers. In the process, they receive payments (at escrow accounts) from customers, pool and transfer them on to the merchants after a time period" (RBI 2020, section 1.1.1, 2).
CPMI	"A payment service provider through which e-commerce merchants can process their payment transactions. An aggregator allows merchants to accept different payment instruments such as credit card, bank transfers, e-money without having to setup a merchant account with a bank, card association etc. The aggregator provides the means for facilitating payment from the consumer to the merchant" (CPMI 2016).
US Chamber of Commerce	"Service provider that allows merchants to process mobile or e-commerce payments. They let businesses accept credit and debit card payments without setting up a merchant account through a bank" (Johnson 2019).
World Bank Group[10]	"A service provider that signs up merchants directly under its own merchant identification number (MID) to process transactions through a single master account. One merchant account is used to represent many merchants opposed to the traditional model which disburses a merchant account to each merchant. It is important to note that aggregators exist also for physical merchants in addition to e-commerce" (WBG 2020, 11).

aggregator, which includes providing e-payment services for paying bills/services" (CBE 2019, 6). In clear contrast with the definitions outlined in table 3, the CBE indicates that a submerchant of a technical payment aggregator "enters into a contract with the technical payment aggregator and the bank"[11] (CBE 2019, 7). Meanwhile, submerchants of a payment facilitator need to have a contract only with the facilitator (CBE 2019, 7).[12]

We can conclude that most regulators and card schemes do not differentiate between merchant facilitators and aggregators. Hence, we will refer to merchant facilitators as the intermediaries that settle transactions on behalf of merchants (submerchants or sponsored merchants). Any reference to merchant aggregator will mean facilitator.

Third-Party Processor

The general term *third-party processor* is used to refer to the entity that processes transactions on behalf of a prime entity within an outsourcing relationship. Mastercard describes a TPP as a service provider that is permitted to provide authorization services, clearing-file preparation and submission, and settlement processing, among other services (Mastercard 2020, section 7.1, 292). Crucially, though, in this definition, a TPP is not permitted to possess, own, and control settlement funds (Mastercard 2020, section 7.1, 292). This is distinct from a payment facilitator. Mastercard's definition of a TPP is similar to the way the World Bank Group has discussed payment processors. In a forthcoming report, the World Bank Group describes a payment processor as an entity that "executes the transaction by transmitting data between the payer, the merchant, the payer's bank (issuing bank), and the merchant's bank (acquiring bank)" (WBG 2020, 11).

Visa's treatment of processors is more complex. It identifies various types of processors, including acquirer processors (Visa 2020, 798), clearing processors (Visa 2020, 810), authorizing processors (Visa 2020, 804), and Visa service-specific processors, such as VisaNet processors (Visa 2020, 885). Its discussion of these processors is high-level and not central to the rules.

US banking regulators use the term *third-party payment processor* in reference to entities that are similar to the definitions of payment facilitator discussed earlier. Table 4 catalogs relevant definitions from the Federal Financial Institutions Examination Council (FFIEC), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Conference of State Bank Supervisors (CSBS). The FFIEC is the examination-coordinating body for the federal banking regulators (Federal Reserve, FDIC, OCC). The Conference of State Bank Supervisors is the coordinating body for American state bank regulators and many nonbank regulators.

These definitions are similar to schemes' and regulators' definitions of payment facilitators, particularly in stressing that the intermediary often uses its own account to process transactions on behalf of merchants. Within this report, ***we will use the definition of international card schemes for TPPs as entities that provide technical services to merchants but not settlement.***

Table 5 catalogs typical functions. A TPP engages in many of the same functions as a payment facilitator. Regarding payment processing, it can be involved in authorization, clearing-file preparation and submission,

TABLE 4: US Financial Regulators' Definitions and Descriptions of Third-Party Payment Processors

Entity	Definition
FFIEC	"Bank customers that provide payment-processing services to merchants and other business entities. Third-party payment processors often use their commercial bank accounts to conduct payment processing for their merchant clients" (FFIEC 2014).
FDIC	"A deposit customer of the financial institution and uses its customer relationship to process payments for merchant clients. The payment processor may use its own deposit account to process such transactions, or it may establish deposit accounts for its merchant clients to process transactions" (FDIC 2014).
OCC	"The processor uses its bank relationship to process payments for merchant clients. Often the processor uses a bank account as the vehicle to conduct such payment processing… the bank often has no direct customer relationship with the merchant" (OCC 2008).
CSBS	"Third Party Payment Processors (TPPPs or processor[s]) originate transactions for consumers or businesses that are not direct customers of the originating financial institution. They provide payment processing services to merchant or business clients and group these payments together to take advantage of economies of scale" (CSBS 2014, 2).

TABLE 5: Third-Party Processor Functions

Functional Area	Function
Merchant onboarding	Take applications and sign up merchants Set up technical mechanism for accepting transactions Customer due diligence Market development
Payment processing	Authorization services Clearing-file preparation and submission Settlement processing (without taking control of funds) Charge-back processing
Security	Fraud control and monitoring
Administrative and relationship management	Statement preparation Customer service Education and awareness

and aspects of the settlement process (Mastercard 2020, section 7.1, 292). Importantly, contrary to a payment facilitator, a TPP never controls settlement funds and does not process transactions on behalf of merchants through its own account. TPPs also play roles in merchant onboarding, security, and administration.

Payment Gateway (for Online Transactions)

Visa and Mastercard do not include substantive discussions of payment gateways in their rules. The most direct definitions of payment gateways come from the RBI, Bank of Ghana, Central Bank of Nigeria, World Bank Group, and Government of Australia. Similarly, although the CPMI does not establish an independent definition of gateways, it lists gateways as a prominent example of a "front-end payment provider," which it defines. Table 6 catalogs these relevant definitions.

These definitions distinguish gateways quite clearly from payment facilitators in the sense that gateways are dedicated to the secure capture, transmission, and receipt of data. As with TPPs, gateways do not handle funds. Rather, they play a role only in the beginning and end of the e-commerce payment life cycle.

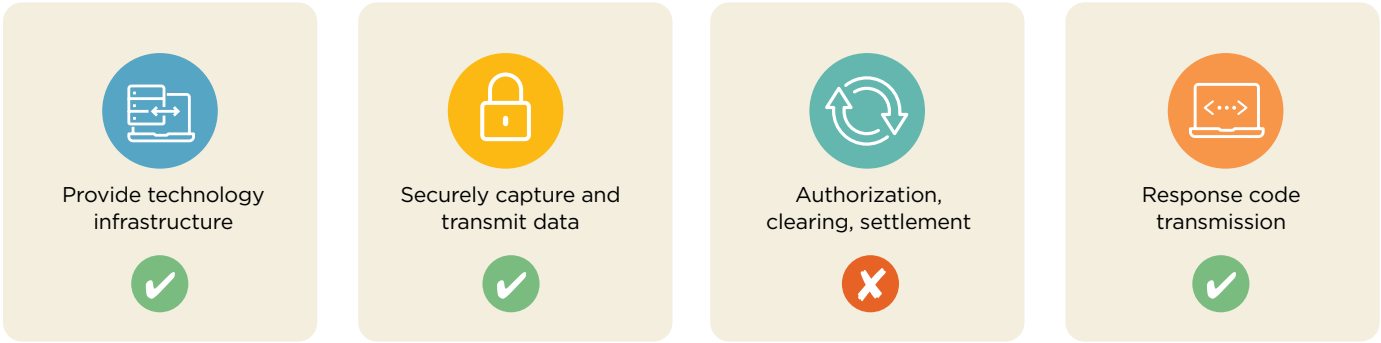
Figure 3 depicts typical payment gateway functions. Gateways provide merchants with the technology infrastructure necessary for secure web-based payment acceptance. Perhaps the most important payment gateway function involves securely capturing and transmitting payment data. Specifically, they receive online transaction data via Secure Socket Layer encryption (Peek 2020), either through a bridge established with the merchant's website or through a gateway's own capturing mechanism, to which customers can be redirected when making online purchases.

Then they securely transmit the data to the next link in the payment-processing chain. In addition, gateways play an important role in formatting data by translating the message format used by the system of capture (for example, internet) to the format used by the relevant network switch (for example, Banknet for Mastercard, Visanet for Visa) whose payments instruments they support. Pay-

TABLE 6: Definitions of Payment Gateway

Entity	Definition
Reserve Bank of India	"Entities that provide technology infrastructure to route and facilitate processing of an online payment transaction, without any involvement in the handling of funds" (RBI 2020, section 1.1.2, 2).
Bank of Ghana	"An e-commerce application service provider that authorizes card payment for e-businesses and online retailers" (BOG 2019, 31).
World Bank Group	"Helps initiate e-commerce transactions or in-app payments. It helps merchants securely transmit the online payment data to the payment processor to continue the lifecycle of the transaction. The gateway is not directly involved in the money flow, but it is a web server to which a platform's website is connected" (WBG 2020b, 11).
Government of Australia	"A service that captures payment information for certain payment methods (usually credit card details) from customers, donors or supporters when they complete a transaction. It creates a message about a transaction in a format that a bank or financial institution can process" (Government of Australia 2012).
CPMI	The CPMI identifies "internet payment gateway providers" as a type of non-bank front-end payment provider, which it defines as "non-banks which typically provide an interface between end users of payment services (payers and/or payees) and the traditional clearing and settlement process. They are mostly present in the pre-transaction, initiation, and post-transaction stages of payment, but usually not in clearing and settlement" (CPMI 2014, 9).

FIGURE 3: Typical Payment Gateway Functions



ment gateways are not often involved in authorization, clearing, and settlement. On the back end, gateways often play a role in sending response codes to relevant parties upon transaction completion (Peek 2020). They also often provide online dashboards that allow merchants to view transactions and take other actions, such as reversals. ***Within this report, we focus on the front-end functions of the gateways, where gateways have direct business relationship with merchants, similar to TPPs, but focusing on e-commerce platforms.*** When the activities of gateways focus only on back-end functions through a relationship with the acquirer, such activities would be out of the scope of this report.

Bill Payment Aggregator

Official definitions of bill payment aggregators are not common, but Visa, the FFIEC, and the South Africa Reserve Bank include discussions of these entities in key documents. Visa, for instance, defines a "consumer bill payment service provider" as a "Merchant that provides a payment solution that allows Cardholders to pay qualifying billers. A biller may or may not be a Merchant" (Visa 2020, section 5.13.1, 476). In the United States region, specifically, Visa further identifies a "bill payment provider" as an "entity that provides a payment solution to facilitate individual or business bill payments on behalf of the Obligee or their financial institution using a Card to pay a biller when the payment is initiated as a bank transfer or cash payment" (Visa 2020, section 4.1.21.1, 228).

The US FFIEC also discusses bill "consolidation-aggregation" as a model of electronic bill payment and presentment.[13] In this model, "the consumer's bills are consolidated by a consolidator acting on behalf of merchants and utilities (or aggregated on behalf of the consumer), combining data from multiple bills and presenting a single source for the consumer to initiate payment."[14] The consolidation-aggregation model stands in contrast tothe "direct model" of electronic billing.[15] Finally, the South Africa Reserve Bank's definition of a "beneficiary service provider" is similar to the notion of a bill payment aggregator and carves out a more direct role for retail

agents collecting payments from payers on behalf of payees. The South Africa Reserve Bank further explains that a "typical example" of this service is "the acceptance of money or proceeds of payment instructions by a retailer or other outlets for payment of utility bills" (SARB 2007, section 1.3.4[a]).

Despite the dearth of official definitions, bill payment aggregators play an important role in facilitating EPA for recurrent payment streams, especially when the billers' own web acceptance platforms are lacking. The types of payments that bill payment aggregators collect include utilities (for example, electric, gas, and water), telecommunication services, financial institution payments (for example, debt repayment), real estate payments, insurance premiums, taxes, and other government fees, among others. Collectively, these constitute a significant share of payments worldwide.

Bill payment aggregators collect payments through a variety of mechanisms, including online portals, mobile applications, and retail establishments, often offering multiple options to customers. Egypt's Fawry, for example, offers "omni-channel" collection through retail establishments, ATMs, mobile applications, and mobile wallets.[16] An added benefit of bill payment aggregators for merchants, to the extent that they offer bill payment collection, is that these services can drive incremental revenue gains and enhance customer loyalty. The key functions of bill payment aggregators include the following:

- Combining data from multiple bills
- Presenting a consolidated payment-initiation platform for payers
- Distributing payments to appropriate payees
- Protecting the security of payment data
- Furnishing payers with receipts
- Performing customer verification in cases where the payee is not a member of relevant acceptance schemes

There are few differences between payments to merchants and billers. Payments to merchants are linked to receiving goods or services on an ad hoc basis, while the relationship between the customer and a biller is typically managed through an agreement. The agreement conditions receipt of a service to payment. Thus, when payment obligations are not fulfilled, delivery of contracted services to the customer could be affected. Another major difference could be the contractual relationship between the facilitator/aggregator and the back-end financial institution. Merchant facilitators typically work through an acquirer, and the acquirer is generally liable for the quality of service provided by the merchant facilitator. A bill aggregator, on the other hand, typically collects funds on behalf of billers, while the back-end bank acts as a fiduciary for funds collection. The fiduciary bank is not responsible for the bill aggregator's service quality. Moreover, often no umbrella agreement, such as scheme rules, governs the bill aggregation process.

Regulators tend to consider the size of the biller or the merchant. While regulators are keen to protect MSMs under financial consumer protection powers, the large merchants or billers might not need to be covered by regulatory measures to protect their rights within their relationship with financial institutions and intermediaries in the same way MSMs need protection. Large merchants and billers generally have their own lawyers and can negotiate and change terms of service with financial institutions and intermediaries. For example, one common model of bill aggregation is for the bill payment aggregator to deposit an initial fund or a guarantee (including a bank letter of credit) with the biller and limit the collection of bills up to the value of the guarantee. By contrast, the terms of acceptance aggregation or facilitation to MSMs may not be fair and may have conditions that discourage EPA by MSMs. These circumstances may require regulatory intervention to protect MSMs.

2.3. THE BASIS FOR REGULATING ACCEPTANCE INTERMEDIARIES

Regulators could have justification to regulate the activities of intermediaries. While there is neither global consensus that requires intervention by regulators nor a single model for such intervention, we nevertheless discuss some of the arguments that underpin the issuance of regulations to govern the operations of EPAIs.

Intermediaries such as payment facilitators and bill aggregators could have access to merchants' and billers' funds. Because facilitators collect payments for goods and services and settle with an acquirer on behalf of the merchants, funds reside in the facilitator account on a temporary basis, creating a settlement risk. The failure by the facilitator to transfer funds to merchants could impair the trust of small merchants and that of society in digital payment services, harming the efforts of regulators to increase the acceptance of electronic payments.

All intermediaries would have access to customers and merchants' financial information, such as account or card numbers, card expiration dates, full names, addresses, and so on. Hence, it might be important for some regulators to control access to and the storage and transfer of such information. Typically, laws and regulations protecting data should apply to all PSPs having access

to financial data, including EPAIs. The rationale for this is that the exposure of data could damage the reputation of the financial sector.

The regulator needs to ensure its ability to apply its measures to all entities engaged in a payment transaction, given that the payment instruments, services, and systems are normally under the oversight of the central bank. Central banks as the payment system regulators can certainly address financial institutions for any lack of conformity with its laws or regulations and will seek the same powers over other entities such as intermediaries, either directly or indirectly. The regulator would need to ensure compliance of all parties to issued regulations and uniformity in practice across all entities.

Intermediaries such as facilitators and gateways actively engage with customers and merchants and, hence, would affect the customer experience. Intermediaries introduce their own technologies and business models to serve the customers and merchants directly. The technologies or business models introduced might be immature and could impair the customer experience or lead to distrust in the service and affect customer confidence in the national payment system. Therefore, regulators may need to intervene to keep the trust in national payment system.

It is in the core mandate of the oversight function to take necessary measures to mitigate risks associated with the national payment system. Risks presented by EPAIs could mainly be operational and financial or general business risks. Such risks could take the form of operational failures due to bad system design, lack of business-continuity arrangements, cybersecurity attacks, and other threats, or financial failures due to business losses, bad investments, or other financial reasons prohibiting intermediaries from providing their services. Because of the positioning of intermediaries in the middle of the processing of financial transactions, it may be important to establish required measures by regulators to mitigate the risks mentioned earlier. Risk mitigation is a core objective of payment system regulators.

Regulators are always concerned with aspects of financial integrity and compliance with customer due diligence requirements. Most intermediaries perform due diligence on their customers. For example, merchant facilitators and aggregators need to perform due diligence on the merchants they acquire. The need for due diligence processes would extend to merchants selling goods or services on the internet, sales that are not executed in a physical location. Merchant due diligence is not limited to the initial enrollment process but is a continuous process of monitoring the merchants' activities.

2.4. APPROACHES FOR REGULATING AND LICENSING ACCEPTANCE INTERMEDIARIES

The report will discuss three different approaches for regulating EPAIs. By *regulation*, we refer to legislative powers delegated to a certain agency (the regulator). Regulators in a jurisdiction have a narrow authority to apply conduct, within their areas of responsibility, that allow them to create and apply the "regulations," rules, or directives. Three approaches for regulating EPAIs are discussed with detail in this report.

Direct regulation: The regulator issues regulations to set controls and limits on EPAIs directly. Regulations will typically be directed at specific types of intermediaries, or they can target certain functions, regardless of the type of intermediary. Upon issuing direct regulations, the authorities will expect any entity providing or anticipating providing such services to apply for a license, authorization, or to be registered. This approach addresses intermediaries directly by specifying the necessary conditions for providing a specific service.

Regulating acquirers and their outsourced services: Where the activity of an intermediary is seen as the responsibility of the acquirer, this activity is considered to be outsourced by the acquirer to a third party. The regulator may issue regulations to the acquiring business. The regulator could issue regulations that address the requirements for outsourcing services in general. Alternatively, the regulator could decide to address specific types of intermediaries as a special type of outsourcing, specifying certain requirements for those intermediaries. The approach of licensing or authorizing intermediaries may differ from one authority to the other. Nevertheless, the acquirer is ultimately liable for the deeds of its intermediaries.

Regulating the payment scheme and system: Regulators may choose to ensure that the scheme governing body or system operator manages all risks within the scheme, including the risks presented by EPAIs. Part of the rationale is that EPAIs are part of a payment scheme or system, such as a card scheme or mobile-payment scheme. As such, scheme or system rules will include the conditions for intermediary service delivery. Within this approach, regulators could apply certain conditions—either general or specific—to intermediaries based on their type. Nevertheless, it would be the responsibility of the scheme governing body or system operator to ensure intermediary compliance with the regulations. Under this approach, intermediaries would not necessarily need to be licensed or authorized by the authorities but would need to be licensed or authorized by the scheme governing body or system operator.

2.5. CONSIDERATIONS IN ADDRESSING REGULATORY AND LICENSING APPROACH

Authorities may elect to use one or several of these three approaches, aligning the approach to the type of the intermediary, types of risks presented, and the overall regulatory environment. For example, a regulator may prefer to consider payment gateways and TPPs as outsourced services that could be supervised by financial institutions. The same regulator, however, may prefer to license and regulate the facilitators directly, preferring a direct approach for the risk of managing customer funds.

Regulators are recommended to use a functional approach, not an institutional approach. In chapter 2 of this report, we clarified the list of functions provided by each entity, and we use the institution type mostly for simplicity. On the one hand, the most distinctive function of a payment facilitator could be collecting funds on behalf of merchants. Hence, we refer to this specific function mostly when referring to the payment facilitators. On the other hand, a certain payment gateway might provide both gateway and fund-collection services through its own account. In such a case, the regulator would treat this entity as performing the functions of both payment gateways and merchant facilitators. It should be noted that, in our report, reference to a specific intermediary means the functions performed by this intermediary as listed in chapter 2.

As the overseer of the national payment system, central banks can achieve their objectives in different ways. The oversight function means that the central bank will monitor the different components of the NPS, assess the risks on participants, systems, and policy objectives, and induce changes on different components of the NPS when required. One oversight instrument of the central bank is issuing regulations. Direct or indirect licensing of service providers could be another oversight instrument. Regardless of the selected approach, the central bank needs to monitor NPS participants closely and clearly understand the risks that those participants present to the NPS. ***The oversight of EPAIs is out of the scope of this report. However, the report's scope covers regulatory approaches as well as licensing approaches.***

The scope of regulations, oversight, and supervision could vary from one country jurisdiction to the other based on legislative structure. For example, some authorities may designate intermediaries as service providers under the supervision and oversight of the central bank. In other jurisdictions, non-bank financial institutions could be under the supervision of a different authority. Such distinction may be relevant within the central bank itself. Within some central banks, the oversight and supervision functions for the PSPs, including intermediaries, are performed by the payment system oversight unit. In others, the supervision of non-bank financial institutions is performed through the supervision unit.

Financial consumer protection and data protection could be the objectives of some central banks. However, in some jurisdictions, the responsibility for these issues may be assigned to institutions other than the central bank. The oversight unit within some central banks may have a specific mandate for protecting the customers within the payment transaction. ***To ensure legal certainty, consideration needs to be given to encouraging innovation.*** Regulators need to issue new laws/regulations, adjust existing legal and regulatory framework, or adapt the existing framework to new products and business models. For example, authorities might need to update existing regulations to address new types of institutions. This is the case of the European Union's update of the Payment Services Directive, as noted in the preamble (EU 2015a, para. 27 and 28). In updating the directive, the European Union was able to put a fence around new PSPs that had emerged, thereby assuring legal certainty. Authorities might issue a general framework that can accommodate technological development. This is the approach taken, for example, in Mexico's fintech regulation, which is crafted in a manner to provide flexibility for a number of areas of emerging innovation in financial technology (Chamber of Deputies 2018).

Furthermore, regulations should be technology neutral. However, some new technologies introduce changes in business models that invite the need for new regulations. Regulations should be oriented to the risks of the business, regardless of the service provider. New types of service providers enhance market competitiveness and should not be disregarded or segregated by regulations. The principle that should be adopted by regulators is "same business, same risks, same rules."[17]

Finally, the level of market sophistication and structure could be an important factor in the selection of the regulatory approach. A market with few dominant providers might require a direct regulatory approach by the central bank. A market characterized by many nondominant providers might be better suited to an indirect regulatory approach. Having strong and mature payment schemes or system operators with detailed rules and clear operational requirements would allow the central bank to apply the existing scheme rules while appending the rules with country-specific conditions.

3. Direct Regulation of EPA Intermediaries

This chapter focuses on the direct regulation of EPAIs, one of three regulatory approaches addressed in this paper. The justification for regulating EPAIs centers on their role supporting financial institutions in the acceptance value chain through processing. Some of the risks associated with their activities include settlement, access to customer funds, operational risks, and those related to customers.

In the direct approach to regulation, the regulation and licensing of EPAIs typically resides with the payment system authority, which could be the central bank or any other conduct authority in charge of non-bank financial institutions and PSPs. In the two other approaches considered in this paper, responsibilities reside with the acquirer in the outsourcing approach examined in chapter 4, while chapter 5 examines the role of the payment scheme and its interactions with EPAIs. In direct regulation, a broader set of responsibilities resides with the regulator. This chapter focuses on the broader role for the regulator—under direct regulation—in addressing the risks presented by EPAIs and corresponding actions that can be taken to mitigate these risks.

This chapter is organized into three sections. The first section details the key elements that must be addressed in the direct regulation of EPAIs. It does so by describing the risks presented by EPAIs, then highlighting regulatory actions to mitigate these risks. The second section examines the licensing and supervision of intermediaries, a process important to ensuring the health of regulated organizations, the protection of investors, and the promotion of market confidence in the ability of an EPAI to conduct business safely and professionally. The chapter concludes with an overview of regulations actually used in practice by some jurisdictions to address some of the identified issues and risks, providing examples of regulations that have been instituted.

3.1 ELEMENTS OF DIRECT REGULATION

Regulators have several reasons to address the risks posed by EPAIs, including to ensure the integrity of a nation's payment system, its reputation, and trust in the system and, in turn, to facilitate the system's continued growth and its underlying economics. This section highlights key risks posed by EPAIs, details the nature of these risks, and highlights potential regulatory avenues to mitigate these risks.

A. Access to Merchant Funds

Some acceptance intermediaries have access to their customer's funds—whether directly through the holding and settlement of funds or indirectly through payments

instructions. There is risk inherent in electronically holding and moving customer funds. These risks compel regulators to establish requirements for the funds' safekeeping. Ensuring the protection of customer funds is critical for maintaining trust in a payment system and, in turn, its efficient operation.

Risk in accessing customer funds can be addressed by setting obligations and controls based on the type of intermediary seeking fund access. Some regulators allow intermediaries only indirect access. In general, an intermediary establishes a merchant account with its partner bank, with the bank treating it as an internal account. The bank shall ensure that settlement to the account is limited to the intermediaries' submerchants and, furthermore, that the intermediary is incapable of disposing the funds for purposes other than settlement with submerchants. In turn, the intermediary needs to establish an account on its platform for each of its submerchants and is responsible for providing settlement to its submerchants through these accounts. The intermediary will typically provide to its partner bank a daily file of transactions to be settled, which the bank will use for releasing funds as the transactions settle. Merchant funds are collected principally by intermediaries, such as payment facilitators, bill aggregators, and gateways having a facilitation role. The concerned intermediaries collect the funds on a temporary basis for distribution to merchants.

Regulators either request intermediaries to deposit funds directly to an account that's under the control of the acquirer or fiduciary bank or allow intermediaries to collect the funds directly in their accounts. Additionally, risks to these customer funds may be further mitigated by requiring merchant funds to be held in an account distinct and **segregated** from the intermediary's funds, ensuring their separation from business funds and thus protecting them from misappropriation.

The timely receipt of funds is critical to merchants, even more so for liquidity-constrained MSMs. Visibility on timing increases the predictability of fund receipt, facilitating financial planning by merchants. Providing time limits for **settlement to submerchant accounts** mitigates these risks.

Some intermediaries require the merchants to keep a portion of the collected funds to protect the intermediaries from credit risks associated to reversal or charge-back transactions. Despite the fact that a request could be justifiable, the amount of requested credit or the length of keeping the credit could be unfair to the merchant. Hence, requirements for mitigating credit risks should be based on quantifiable risk measures, with consideration to transaction size, the nature of a merchant's business, and reversal or charge-back rates.

Another area of concern with respect to merchant funds is advance payment, in which customers make payment to a merchant before the receipt of goods or services. Risk stems from a merchant not fulfilling its obligation in a transaction. Examples include travel-related payments, the online purchase of goods, and some services. To address the risks of these asynchronous flows, intermediaries may hold funds associated with a purchase in escrow, providing settlement once orders are fulfilled. Another mechanism is for the EPAI to hold reserves—a percentage of a merchant's electronic payment proceeds. Reserves can be adjusted based on the nature of the risk environment. During the COVID 19 pandemic, reserve requirements trended higher because of increased risks, putting pressure on merchants with low liquidity.

B. Access to Customer's Financial Information

Several trends are making customer information more accessible. The types of customer data available have proliferated, and the ability to capture, transmit, and access such data through new channels has increased. This information includes customers' personal data, merchants' business data, and transactional and financial data, including card numbers and account numbers, among others. In addition, new applications of customer data are being developed along with associated business models, such as customer-centric payment services, such as account information service providers, which are able to aggregate data from consumer payment accounts using interfaces, enabling them to have an overall view of a consumer's financial situation at any moment (EU 2015a, para. 28). Other applications include credit scoring, know-your-customer solutions, and efforts to minimize fraud. In fact, data has become a critical component of new capabilities and business models and has the potential to change the economics of payments—further enhancing the ability of providers to reach the marginalized and excluded.

Data trends, for example, are helping to spur payment innovation, in turn enabling the inclusion of more MSMs. Nevertheless, these trends raise issues that reinforce the need for measures to protect the financial information of EPAI customers. For example, how do we address the processing, transmission, and storage of data used to derive value in new solutions and business models? What are the implications of regulating data for the entrance of new players into the market, both local start-ups and established global entities? These are just a few of the questions raised by current data trends.

Data Protection

Customer financial data captured by EPAI must be protected. For example, data that is retained and stored

must be protected from those who seek to compromise the integrity of the intermediary's systems. This requires the data—which, in some cases, is becoming more concentrated with outsourced providers—to be stored safely. Data must be safely captured and transmitted to participants across the acceptance value chain, with risk mitigated through security measures and standards for its capture and transmission. Furthermore, permissible uses of customer information must be established—discussed in more detail below—to ensure that the rights of data ownership are recognized, and that protocols associated with ownership rights are clearly understood, ensuring the legitimate and sanctioned use of customer financial information. Data breaches have become a greater concern as more data becomes electronically available. In general, privacy risks have increased as the number of customers served by a provider increases. These risks can be compounded if the provider possesses other types of data that has been linked to customer financial information. These risks may emanate from services provided directly to merchants or services provided to an intermediary by an outsourced provider (WBG 2019).

Security Measures and Standards

Service providers need to ensure that data captured in customer interactions is done so in a secure manner. Industry standards provide a mechanism for enhancing data security. **PCI-DSS** (Payment Card Industry Data Security Standard) is a body of standards established by major card schemes to secure card transactions against data breaches, theft, and fraud. Meant to safeguard this sensitive information, it sets standards and associated security measures for the capture and transmission of data by organizations that process payment transactions. This includes, for example, standards to encrypt the transmission of cardholder data.[18] A separate industry standard, **PA-DSS** (Payment Application Data Security Standard), is meant to ensure that payment applications are secure. The protection of data can be assured only when all players within the payment ecosystem maintain best-in-class security standards (Mastercard 2017). These standards address the increased complexity of the acceptance value chain, extending data security standards to mobile payment-acceptance applications associated with schemes.

Permissible Use of Customer Information

Easier access to customer data is creating new opportunities for innovation, but its misuse by intermediaries is also a source of risk. Data has been critical in supporting innovation and the development of new business models, including credit scoring, fraud applications, and expanded customer-centric solutions that incorporate payments, such as those increasingly being used in sectoral approaches, such as agriculture. These innovations can improve the value of payment solutions to merchants and small businesses, support more use cases, and drive system efficiency through greater usage.

EPAIs must ensure that they use data in a permissible manner. This requires abiding by use rights that may be explicitly addressed by regulators. These rights might include the use of customer data to validate funds availability for the authorization of payment transactions and for fraud mitigation.[19] More broadly, fundamental issues of data ownership have been raised in recent efforts to regulate payments. While these issues may not directly affect EPAIs at this moment, they may be relevant going forward, as intermediaries and the services they provide continue to evolve. Some of these issues include ownership rights around data and the implications for how data can be used. These rights need to lay out the **permissible uses** of this data to ensure its proper use, so as to protect consumers, merchants, business partners, and intermediaries—for example, open banking models where the ownership of customer data has shifted from financial institutions to customers. Hence, it is the customer who possesses the right to share data. Some regulators are requiring institutions in possession of customer data to obtain the consent of customers before the institutions may use this customer data.[20]

C. Consumer and Merchant Protection

EPAIs are well positioned to focus on MSMs, in turn helping to advance financial inclusion. Their customers and the customers of their customers tend to be relatively new to digital payments, not completely familiar with these services and the details surrounding them. The situation reinforces the importance of protections for EPAI customers that are necessary to instill and reinforce trust in the payment system.

Transparency about charges is essential to the predictability of cash flows and informing business decisions. Not only do many EPAIs' merchants serve poorer populations, but they, too, are often poor, struggling to manage their cash flows, reinforcing the need for information about pricing and charges to be transparent and predictable—minimizing the risk of surprises.

Consumer protection is needed in the form of approaches for managing the resulting complaints in a manner that is fair and equitable. Mistakes, both human and system generated, are inevitable, as are misunderstandings over the execution of transactions. Minimizing the impact of these inevitable errors will provide a better payment experience, enhancing the utility of electronic payments.

Regulations addressing complaints can include the following elements: approaches and procedures for the effective handling of customer grievances, complaints, and disputes; protections for unauthorized and incorrectly executed transactions; designation by EPAIs of an individual responsible for the complaints process; and efforts to raise awareness about customer protections and the corresponding process for recourse.

General consumer precautions are another avenue of regulation to protect consumers and merchants. Broad protections can be delineated and made more explicit. One example is the delineation of consumer liability under various scenarios. Another is the application of technical neutrality, ensuring merchant protection regardless of payment instrument or business model used.[21]

D. Management of Risks

As information- and technology-centric businesses, EPAIs present a number of broad overall risks. These risks require a risk-management framework as well as regulations for mitigating business, operational, and IT security risks.

General Governance and Risk-Management Framework

The licensing and registration process under direct regulation generally has mechanisms in place for EPAI applicants to demonstrate the competent governance of their firms. Competent governance helps to ensure the entities' efficient management and operations. In addition, good risk management requires a framework to guide this activity within the management of risks to the firm. This too can be a requirement in the licensing process, with applicants demonstrating, for example, competence through the possession of a robust risk-management framework.

EPAIs face general business risks stemming from their business strategy and marketplace activities. These include decisions about market positioning—namely, the customer segments they have chosen to serve and the solutions they offer, which might include a movement beyond their core focus and their chosen business model. Some intermediaries, for example, may focus on riskier merchant categories. In addition, there may be financial risks stemming from losses in investments made to support these activities or the inability of the intermediary to continue its business or smoothly shut down due to financial problems. Finally, negative impacts on an intermediary's reputation can create business risk. Threats or dangers to the name and standing—to the **reputation**—of an intermediary stem from the inability to provide reliable service or address issues in a timely manner, the disclosure of confidential information, and incidents stemming from the failure to address adequately the risks inherent in an information-based business moving people's money.

Operational Risks

Risks stemming from the operation of an intermediary and its underlying technology need to be mitigated. Intermediaries need to execute transactions accurately and in a timely manner. This requirement leads to operational risks stemming from the **potential interruption in the continuity** of an intermediary's operation as well as the intermediary's inability to recover from a disaster. EPAIs should undertake business-continuity planning, ensure proper systems are in place, and demonstrate the ability to address potential threats. The need to address failures in business continuity though **disaster-recovery planning** requires a demonstrated set of policies, tools, and procedures to be put in place to enable the recovery or continuation of vital technology infrastructure and systems.

Another dimension of operational risk is the need for intermediaries to meet the criteria laid out in their service-level agreements. The increased complexity of coordination efforts across the payment value chain is just one element complicating these efforts. For example, EPAI service-level agreements may stipulate the elapsed time to onboard and provision an MSM for payment acceptance.[22]

Other operational risks, such as IT, expose an organization's critical technical assets (for example, computers, networks, and data) to unauthorized access. These risks typically stem from the lack of robust technical infrastructure and associated standards necessary to support efficient business execution. Robust infrastructure and standards can minimize risks of technical failure and unexpected acts (for example, attacks, piracy, and fraud).

To remediate these risks, EPAIs must understand their IT assets and the nature of risks posed to their assets, enabling the identification of gaps and their remediation. Such actions can help to protect information assets by helping EPAIs understand and address their vulnerabilities. Furthermore, organizations must be aware that these risks are not static and, instead, are continually evolving—necessitating a process to make appropriate upgrades in response to developments, as necessary. One remedy is to require organizations to become **certified ISO 27001** providers. Organizations that meet the standard's requirements can choose to be certified following successful completion of an audit by an accredited entity.

The storage of increased amounts of data and its potential access by outside parties present a unique **cybersecurity risk** to EPAIs. This risk stems from potential attackers seeking unauthorized access to data that may be located

on an EPAI's infrastructure, computer networks, and information systems. The expansion of channels available for data capture and transmission raise additional cybersecurity considerations—including navigating its increased complexity.

E. Compliance

Compliance requires EPAIs to fulfill rules or standards to address risks external to their operating environment. Compliance with regulations and laws may be addressed through policies or procedures. Merchant onboarding encompasses several activities across the acceptance value chain, including the solicitation of merchant applications, due diligence and enrollment, and, finally, merchant setup, training, and acceptance provisioning. During the onboarding process, it is critical for EPAIs to validate the identify of their potential merchant customers as well as address other critical decision points. They must validate business ownership through know-your-customer efforts and collect information necessary to ensure proper setup of the merchant's account. Proportionate risk-based approaches can be deployed to address the risks of onboarding, which could be designed so that they place less onerous information requirements on low-risk merchants.[23]

As part of the onboarding process, EPAIs must address and mitigate risks stemming from the potential for money laundering and the financing of terrorism. Yet a balance must be achieved between the risks of money laundering and the financing of terrorism and the need to financially include the MSMs. A risk-based approach, including simplified requirements for low-risk merchant categories and through applying transaction limits and usage restrictions (WB 2005; FATF 2013), can minimize risks of money laundering and the financing of terrorism while propelling the growth of MSM acceptance.

Market Competitiveness

Competitive markets are important because they provide consumers with greater choice. Regulators can ban exclusivity agreements between intermediaries and service providers as well as between intermediaries and merchants to support competition and increase options for participants. Furthermore, regulators can put forth reasonable prudential requirements, such as capital requirements, that reflect risk, ensuring easier market entry. These actions support an expanded choice set that stems from the innovation and competitive prices that characterize such competitive markets and could, in turn, facilitate greater financial inclusion by enabling the viable extension of financial services to difficult-to-reach underbanked and unbanked populations.

A level playing field is required that does not favor one particular type of entity—new or established—to ensure a contestable and competitive marketplace.[24] When the playing field is not level, there is a risk that new entrants—not only small providers but also large players—can arbitrage regulation, because, as new entrants, they are not subject to the **same level of regulatory scrutiny** as established players (WBG 2019). Given these risks, efforts should ensure that the playing field remains level for both current and potential entrants. A level playing field helps to guide actors by providing proper signals, ensuring that incentives are not distorted to support balanced innovation and a competitive market environment (Mastercard 2017). Market competitiveness is a market-wide objective, and its implementation is generally addressed through general competition laws. However, there are cases in which a regulator has sought to address competition specifically through narrowly focused provisions. For example, this was done by including limits on funds that EPAIs may keep on behalf of their clients.[25]

F. Managing Outsourcing Risks

Firms outsource activities for several reasons. These include the ability to offer innovative services, reduce costs, or address new market segments. Outsourcing certain activities—especially those that cannot be provided competitively—can reduce fixed costs, effectively lowering market entry costs and, in turn, supporting new entrants and increased competitiveness. Outsourcing by EPAIs creates risks that regulators need to be aware of, understand, and establish measures to mitigate. In direct regulatory regimes, regulatory efforts focus on addressing outsourcing by EPAIs. EPAIs may need to outsource some of their functions. Activities outsourced by EPAIs can include merchant enrollment, IT, and data storage, among others.

Regulation pertaining to the auditing and supervision of EPAI outsourcing may include requirements for auditing EPAIs as well as entities to which they, in turn, may have outsourced activities. One such area is data storage and the risks presented by outsourcing this function, such as the security of data. This issue was raised in the section on cybersecurity. One potential challenge is the amassing of market power by outsourcing partners. This can occur from specialization and consolidation among providers serving EPAIs—cloud-storage services being one example (Khiaonarong and Goh 2020; FSB 2020). Increased market power by service providers may also make it more difficult for an EPAI to switch service providers and raise issues regarding the provision of back-up services. Concentration may raise the potential for systemic risk, where a failure of a service provider may lead to a failure of the service provided by multiple banks through this service

provider. Finally, increased specialization by providers associated with concentration requires regulators to possess the necessary technical skills to address service provider processes fully. **Regulatory purview and access are critical to ensure that regulators are able to exercise their authorities.** An outsourcing provider may fall outside of a regulator's purview because the provider is not subject to its regulation. The lack of purview prevents regulator access necessary to assess risks of their service providers properly. Risk arises when, for example, a regulator has no physical access to stored data or its processing (WBG 2019). Hence, care must be taken in crafting regulations to ensure that these providers do not fall outside the regulator's purview. Alternatively, the regulator can require clauses in contracts between EPAIs and their outsourced providers that stipulate the right of the regulator or any delegate to audit the outsourced entity.

3.2 AUTHORIZATION OF INTERMEDIARIES[26]

Under a direct regulation regime, authorization can be provided by licensing, registration, or even notification. This authorization is typically granted to EPAIs by the financial-sector authority. In managing the authorization process, the authority establishes guidelines and oversees and supervises the PSP.

In the authorization process, intermediaries must typically meet several macro prudential requirements intended to mitigate risks. These requirements protect consumers and ensure the financial health of firms, promote market confidence in the soundness of acceptance intermediaries, and ensure the ability of EPAIs to conduct business safely and professionally. Requirements can potentially encompass several important dimensions of the applicant seeking authorization—for example, demonstrating that the applicant is a viable business entity with adequate capitalization or showing that the firm is properly governed. Often addressed through fit-and-proper requirements, these ensure the sound, capable, and prudent management of the business. Furthermore, the regulator may require a risk-management framework from the applicant, in which the risks faced by the firm are identified and approaches to their remediation are spelled out. **Requirements for authorization by regulators should be proportional to the risks presented by the EPAI.** Capital requirements, for example, should be proportional to the financial and operational risks; intermediaries processing larger volumes should be required to meet larger capital requirements. Singapore pursues a risk-based approach, requiring different licenses with corresponding obligations based on processed amounts. Ghana established capital requirements based on the type of intermediary seeking license. Many authorities set the capital requirements based on the nature of the business and the size of operations.

Supervisory elements associated with licensing can include controls and contractual requirements. In the licensing process, the regulator can stipulate controls in the granting of the license. These controls, for example, might carve out areas of permissible operation for the intermediary, such as permitted merchant categories or limits on the size of merchants that can be served. In addition, mechanisms to facilitate monitoring of the delineated controls can be established as terms in the EPAIs licensing. Another vehicle is for the regulator to stipulate elements to include in contracts with participants across the acceptance value chain. Contracts with acquirers might stipulate terms regarding permissible merchant turnover. In addition, service-level requirements can be established, including those related to client onboarding as well as other aspects of the onboarding process related to customer satisfaction and retention. Moving along the acceptance value chain, regulators may require contracting provisions be included in outsourcing agreements, to address concerns about supervision and audit, thereby ensuring that risks are addressed. For example, a right-to-audit clause can ensure access and effective monitoring, to enable the regulator to conduct security audits on the outsourcing provider (RBI 2020).

Terms can also be included by EPAIs in their contracts with merchants. Agreements may explicitly require merchants to undertake activities to comply with standards, such as PCI-DSS and PA-DSS. In addition, agreements may address data access in general by requiring merchant agreements to include provisions for the security and privacy of customer data (RBI 2020, article 7.5). Finally, agreements can seek to limit risks associated with exposure as well as to ensure compliance. The latter may include graduated requirements of anti-money-laundering/combating the financing of terrorism guidelines, placing limits on acceptance through the imposition of caps on daily transactions and volumes.

3.3 EXAMPLES OF REGULATORY MEASURES

This section highlights some of the ways in which regulation can be crafted to address the risks presented by EPAIs. It does so by identifying the objective of regulations that have been instituted and provides some examples of regulations from research on a number of countries. The focus in the last two sections is on selective risks presented by EPAIs, including customer protection, access to customer funds, access to customer financial information, outsourcing, and the authorization of provider licenses. Finally, the merits of these regulations are discussed.

BOX 1

CASES OF DIRECT REGULATION OF EPAIs

The box highlights several examples of the direct regulation of EPAIs, including Ghana, Thailand, Singapore and the American state of Georgia.

Ghana

The Bank of Ghana (2019), in addition to covering merchant acquirers, explicitly addresses payment gateways. The bank's definition of a gateway is consistent with the definition established in chapter 2 of this report; in addition, some standard security requirements for gateway operation are stipulated (BOG 2019).

Ghana has separate licensing standards for acceptance intermediaries. Thus, the Bank of Ghana takes a direct approach to intermediary regulation. In its "License Categories and Permissible Activities," the Bank of Ghana outlines permissible functions of various classes of "Payment Service Providers," which perform intermediary activities, including "merchant aggregation," "payment processing," "biller/merchant aggregation," and "third-party payment gateway services," among other activities (BOG 2020). In Ghana, PSP licensing is mandated by the Payment Systems and Services Act of 2019 (Republic of Ghana 2019).

Thailand

Acquirers, payment facilitators, and other payment service businesses that provide "a service of receiving payment on behalf" must be licensed with the Ministry of Finance (Kingdom of Thailand 2018; BOT 2018e). Acquirers and acceptance intermediaries are subject to a similar regulatory regime in Thailand. Thus, Thailand takes a direct approach to the regulation of intermediaries. The Bank of Thailand's payment services regulations (BOT 2018e) and licensing instructions (2018b) set out a variety of standards for acquirers and acceptance intermediaries. No distinction is made between bank and non-bank acquirers in Thailand's standards; presumably, they apply to both. Thus, in addition to regulating acquirers, Thailand takes a direct approach to regulating acceptance intermediaries.

Singapore

Singapore's Payment Services Act of 2019 sets out an activities-based, risk-based, and right-sized licensing regime for certain payment services, including merchant acquisition services (Republic of Singapore 2019). The act sets out two types of licenses—a standard payment institution (SPI) license and a major payment institution (MPI) license. SPI licensees cannot process more than $3 million in payments per month and are subject to capital requirements. MPI licensees have no payment-processing limits and are subject to higher capital requirements than SPIs. The act also sets out risk-mitigation standards for merchant-acquisition services in the areas of user protection, interoperability, and technology and cybersecurity (Republic of Singapore 2019). Interestingly, licensees providing merchant-acquisition services are not regulated for compliance with anti-money-laundering/combating the financing of terrorism requirements (Republic of Singapore 2019).

Banking institutions, including merchant banks, are not subject to the Payment Services Act because they are already subject to a regulatory regime under the Banking Act. The Monetary Authority of Singapore indicates that banks and payment institutions are generally subject to similar requirements (MAS 2019b).

American State of Georgia

Some states in the United States have direct regulatory or at least licensing jurisdiction over EPAIs. This is the case for the state of Georgia, which has developed a specialized charter for merchant acquirer limited purpose banks (MALPBs). The charter allows MALBPs to access payment card networks directly, without the sponsorship of another regulated financial entity. In addition, it sets out a number of requirements for MALPBs. PayPal and Square are licensed by the Georgia Department of Banking and Finance as MALPBs.[27]

Access to Customer Funds

Setting obligations and controls is a means to ensure the proper access by intermediaries to customer funds. Intermediaries typically need to open accounts with a bank—which are treated as internal accounts of banks—to facilitate their collection of payments from customers and merchants. One control is for regulators to require banks to ensure that such accounts are not maintained and operated by intermediaries.[29] Regulators often require payment facilitators to have an escrow account with a commercial bank in which they hold collected funds. A regulator may treat the intermediary as a designated payment system (service provider).[29]

Two approaches to the treatment of funds settlement were observed. One treatment focused on process. This explicitly grants some intermediaries the right to perform settlement and requires controls in the form of processes and procedures (Indonesia). A second approach is outcome based and provides guidance on the timing of settlement. An obligation on settlement timing implicitly recognizes that intermediaries conduct settlement through accounts they manage directly or indirectly. The net effect of an approach focused on timing is to provide greater predictability of funds flow. Such predictability is critical for financial planning by customers, especially micro and small businesses that may face liquidity constraints.

The risks associated with access to customer funds compels regulators to establish requirements for the treatment and safekeeping of funds by EPAIs. Intermediaries are generally obligated to segregate customer funds into separate accounts for safekeeping. A regulator may extend these obligations by stipulating requirements for access to customer funds, should an intermediary become insolvent. A number of regulators have addressed the treatment of payments made before the delivery of goods or services. One approach to minimize the risks stemming from asynchronous activities is to require intermediaries to maintain reserves in an escrow account with a commercial bank (India). Though an EPAI is not the owner of funds in the escrow account, the intermediary can influence the movement of funds to and from the account. Finally, while not observed in our review, a regulator could require an intermediary to hold other types of guarantees with its bank partner.

Access to Customer Data

Regulators have established requirements for access to customer data to ensure the protection of EPAIs and their customers. The focus of these requirements is to ensure the safety of customer data as well as its legitimate and sanctioned use. While beyond the scope of this paper, changes are emerging with respect to the underlying ownership rights associated with customer data. These changes are arising, in part, in response to innovation that provides new ways and business models for the use of payments data, including open-banking application programming interfaces.[30] The questions raised by the use of customer data will become increasingly relevant to EPAIs as they continue to evolve their service offerings.

The key questions concerning customer data currently addressed by regulators with respect to EPAIs focus on access and legitimate use—namely, how is access provided, and when is access granted? More specifically, what are the sanctioned uses of customer data? Regulators have addressed access in several ways. One is to address the technology used in providing payment services, even highlighting technologies that could be used for customer authentication (Chamber of Deputies 2018). Another approach focuses on merchant agreements, requiring the inclusion of provisions for the security and privacy of customer data (RBI 2020). Two explicitly permitted uses of EPAI customer data were observed in the reviewed regulations: access to customer data to validate funds availability for the authorization of payment transactions (PSD2, article 65) and its use in fraud mitigation (PSD2, article 94) (EU 2015a).

Going forward, some regulators may continue to recognize individuals' enhanced ownership rights over their personal data. Some changes are arising in response to innovation brought by fintech and developments in open banking, both of which leverage payment system data and new types of intermediaries.

The developments in data use highlight a trade-off between enabling innovation—with its potential of increasing inclusion through improved economics—and providing individuals with greater control over their data through the rights of ownership. It is important to structure rights and permissible uses in a manner that complements continued innovation; the challenge lies in achieving the optimal balance.

Customer Protections

Several approaches by regulators for protecting customers were observed; they differ primarily in breadth and area of focus. For example, regulations addressing complaints might include some of the following elements: approaches and procedures for the effective handling of customer grievances, complaints, and disputes (RBI 2020; BI 2016; Chamber of Deputies 2018); extending protections to both unauthorized and incorrectly executed transactions (EU 2015a); requiring EPAIs to designate a responsible individual for the complaints process (RBI 2020); and efforts to raise awareness through education. The RBI in 2020 established the need for EPAIs to develop a policy to address complaints by payment ser-

vice users. Bank Indonesia in 2016 focused more broadly on the need to provide customer protections (BI 2016). Regulation issued by the RBI in 2020 focuses on awareness and education, seeking to ensure customer access to provider policies through several channels, including websites and mobile applications.

A broader approach to customer protections might require the development of a dispute-management framework. This could include customer redress, to ensure the resolution of disputes, as well as the appointment of an officer to be responsible for handling customer grievances (RBI 2020). A clear delineation of roles and responsibilities around actions necessary to protect customers could be detailed in contracts between stakeholders (RBI 2020).

A more specific regulatory approach spells out afforded customer protections. For example, the European Union clarifies liability in a several scenarios. This includes unauthorized and incorrectly executed transactions—with liability for unauthorized transactions, their correct execution, and the burden of proof for fraud and negligence assigned to the service provider (EU 2015a, article 71). Other afforded protections can include providing customers with clear information, transparent pricing, and, finally, spelling out protections afforded to accepting merchants.[31] In addition, there are stipulations for incident reporting when personal data is compromised (India). Other regulators may refer to separate legislation that comprehensively spells out rights of financial services users. This is the case in Mexico, where consumer rights are detailed in the Law for the Protection and Defense of the User of Financial Services.

Outsourcing

In direct regulatory regimes, regulatory efforts address outsourcing by focusing on the activities and contractual arrangements of EPAIs. Regulators recognize the need for EPAIs to outsource some functions to support their operations. An option for mitigating these risks is for the regulator to make an EPA fully liable for the actions of their outsourcing partners. This stipulation would provide the incentive for additional vigilance on the part of EPAIs and, in turn, provide additional protection to their bank partners.

Outsourcing arrangements may already exist at the time authorization is sought by an EPAI. Alternatively, they can be entered into after their licensing. If outsourcing is being pursued at the time of provider authorization, the regulator may require the applicant to provide additional details on the nature of the proposed agreements. This could include the provision of an outsourcing policy document that addresses, among other things, security aspects. One regulator requires that an EPAI to indicate in such a document "how they ensure a high level of technical security and data protection, including for the software and IT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations" (EU 2015a, article 5.1). More commonly, EPAIs may enter into outsourcing arrangements after they have been licensed. Most regulators require financial institutions and EPAIs to abide by existing outsourcing regulations. These typically require an EPAI to report about their outsourcing arrangements to the regulator. Several regulatory provisions were observed with the goal of addressing concerns about supervision and audit. These provisions focused primarily on the inclusion of clauses into contractual agreements between EPAIs and their outsourcing partners as a mechanism for mitigating risk concerns. For example, in this regard, the RBI states that "*there shall be an outsourcing agreement providing 'right to audit' clause to enable the entities/their appointed agencies and regulators to conduct security audits. Alternatively, third parties shall submit annual independent security audit reports to the entities*" (RBI 2020, annex 2, 1.17).

Motivations for including clauses in EPA outsourcing contracts may differ. A right-to-audit clause can ensure access and effective monitoring to enable the regulator to conduct security audits on the outsourcing provider (RBI 2020). Other regulators may be particularly concerned with recourse and legal purview. Regulators need legal recourse to oversee relevant activities of outsourced providers. Recourse can be addressed by contractual clauses between EPAIs and outsourcing providers. For example, a regulator may require bank contracts with intermediaries to specify the need for bank approval of intermediary efforts to outsource activities authorized in their contract.

Yet another nuance in the motivation to include contractual clauses is ensuring effective monitoring. In this case, the regulator may stipulate a clause requiring that the outsourcing of important operational functions does not impair internal controls or the ability of authorities to monitor compliance. For example, this has been the case for the outsourcing of data-storage capabilities, which raises a number of concerns for regulators. These various treatments of outsourcing—in a direct regulatory regime—put the responsibility squarely on the intermediary. As such, they are distinct in focus from indirect regimes, where the burden is put directly on the acquirer.

Authorization of Provider Licenses

The decision to authorize an EPAI depends on the applicant demonstrating that its business is sound, well run, and able to address the risks presented by the services

it intends to provide. When risks presented by the PSPs' activities are minimal and have not warranted licensing, registration may prove sufficient, thus providing the regulator with a means for monitoring development (EU 2015a, para. 47). This view is echoed by the Bank for International Settlements, which notes that non-banks may be licensed, but that they can also be registered with appropriated authorities if the risk associated with the intermediaries' activities do not warrant licensing (CPMI 2014). Regulators, however, must be careful not to put forward too many licensing categories, as this could result in a loss of regulatory clarity. This section touches on some of the authorization requirements being used by selected regulators in the licensing of EPAIs.

A key requirement for authorization is an applicant's demonstration of its financial stability. Capital requirements are a common approach for ensuring stability. They should not reflect a one-size-fits-all approach but, ideally, should be tailored to the activities of intermediaries and their risks. Regulators may want to consider the use of a guarantee, such as indemnity insurance, in lieu of capital.

Authorization commonly requires a demonstration by the applicant of effective governance together with fit-and-proper management of the firm. Several approaches with varying levels of rigor have has been observed for instituting this requirement. One requirement is to possess a board of directors (Chamber of Deputies 2018). Other regulators (for example, Bank Indonesia) consider the competence of the parties (BI 2016, article 13). Still others (for example, in the European Union) require a description of governance arrangements (EU 2015a, article 5e). Regulators can also seek additional input by reaching out to external parities to get their views on the capability of the applicant's management (RBI 2020, article 5.1). Regulators may also require applicants to submit a business plan and a feasibility analysis regarding their intended activities.

Management of Risks

In addition to the two common requirements for sufficient as well as effective governance and management, regulators may require intermediaries to satisfy additional requirements related to their ability to manage risk. A regulator may require applicants to submit an overall risk-management framework, or they may stipulate the need for a technology framework. These requirements should not be viewed as static. Given market innovation, some regulators have put forward updates, for example, to the authorization process to address new risks that have emerged. For example, the European Union's revised Payment Services Directive (PSD2) included updates that sought to enhance the level of payment security—namely, requiring a security policy document as well as a description of procedures for managing security incidents, contingency procedures, and so on.[32] Another example is requiring PSPs, as a general rule, to apply strong customer authentication (EU 2015a, article 97).

4. Regulating Acquirers and Their Outsourced Services

This chapter focuses on a regulatory approach to EPAIs that treats them as outsourcing providers to merchant acquirers. The focus in this approach is on regulating an acquirer's outsourcing actvities—in effect, an indirect, rather than direct, approach to regulating an intermediary.[33] Addressing acquirer outsourcing takes up the activities of intermediaries. Acquirer regulation is first addressed to provide context and a point of departure to examine the regulation of acquirer outsourcing.

The chapter is organized into three sections. Section 1 lays the groundwork by highlighting relevant themes in acquirer regulation. Section 2 reviews the motivation for acquirer outsourcing, associated risks, and their mitigation. Section 3 focuses on authorization of acquirer outsourcing.

4.1 REGULATING MERCHANT ACQUIRERS

In many jurisdictions, regulators generally exercise direct authority over acquirers by enforcing acquirer regulations. Acquirer regulations tend to address the types of permitted acquirers, their responsibilities and obligations, minimum macroprudential and functional requirements, governance, and their obligations for outsourced services. In some cases, that latter includes specific obligations regarding EPAIs.[34]

Acquirers are required to manage different types of risks. The Bank of Thailand mandates a board-approved risk-management policy for acquirers. The RBI requests that acquirers seek board approval for a policy statement regarding their approach to merchant acquiring. Several regulators, such as the Bank Negara Malaysia (BNM), RBI, FDIC, and OCC, stress the need for acquirers to perform adequate merchant due diligence, training, and transaction monitoring. US regulators focus on the merchant underwriting process, including review and approval of merchants, identification of prohibited or restricted merchants, and charge-back monitoring. The US state of Georgia requests acquirers to have a chief risk officer responsible for measuring, monitoring, reporting on, and controlling risks inherent in payment processing, including operational and technological risk, credit risk, liquidity risk, legal and compliance risk, reputation risk, market risk, and strategic risk, among others.

Many regulators, such as the RBI, give specific attention to IT risks, including setting standards such as PCI-DSS for acquirers. Some regulators may require the adoption only of robust IT and data security standards. The BNM requires an acquirer to manage the risks presented by its technology and technology operations (for example, data center infrastructure and operations, network resilience, third-party service providers, cloud services, access con-

trol, and the security of digital services) and to manage its cybersecurity risks. Furthermore, regulators generally stress the need to manage fraud risks and also to enforce dispute-resolution measures.

Regulators may allow non-banks to act as acquirers. Non-bank acquirers are direct participants in card schemes; hence, they may have access to the card scheme's clearing and settlement functions as well as full liability for merchants' funds. Due to the lack of access to the domestic or international settlement systems, many non-bank acquirers use the services of a commercial bank to act as their settlement bank. A non-bank acquirer will need to be an authorized member of the card schemes they support, but some jurisdictions may also require them to be registered or licensed by the domestic regulator. Regulators may issue regulations for non-bank acquirers, while no similar regulations exist for bank acquirers. As they are not credit institutions, the risk of greatest concern regarding non-bank acquirers is their ability to manage credit risks associated with merchants and adequate settlement of merchants' accounts. Hence, regulations for non-bank acquirers put emphasis on prudential requirements and credit risk mitigation.

The regulation of outsourcing by merchant acquirers can vary for EPAIs. In addressing outsourcing to intermediaries, some regulators may take a general approach by establishing general rules for outsourcing financial services. Furthermore, they may treat intermediaries as TPPs of acquirers. As a result, no specific regulations are developed for intermediaries. Therefore, only general outsourcing rules apply to them. Other regulators may choose to issue regulations specifically addressing the outsourcing of activities to EPAIs.

BOX 2

REGULATING MERCHANT ACQUIRERS

This box highlights key aspects of merchant acquirer regulations, proposed regulations, and supervisory standards in several jurisdictions. Where relevant, interactions with intermediary standards are highlighted, as well as observations on their implications for the regulation of outsourcing activities. The markets examined are Nigeria, Malaysia, the United States, India, Indonesia, the American state of Georgia, and the European Union.

Nigeria

The Central Bank of Nigeria has issued the "Regulatory Framework for Non-bank Acquiring in Nigeria," which spell out roles, responsibilities, and other requirements for merchant non-bank acquirers (CBN 2021).

The central bank's framework regulates aspects such as requirements for merchant agreements, merchant underwriting, merchant risk monitoring, third-party agent risk, settlement arrangements, and risk management, among other factors.

In a number of cases, the regulatory framework of the Central Bank of Nigeria directs non-bank acquirers to adhere to card scheme rules.

Malaysia

The Bank Negara Malaysia (BNM) has issued a policy document detailing the regulatory requirements for proposed detailed regulation of registered merchant acquirers, covering governance, operational requirements, and IT security controls (BNM 2021). Malaysia's proposed regulations apply to both bank and non-bank acquirers. Furthermore, the policy document's proposed regulations outline specific capital requirements for non-bank acquirers (BNM 2021, article 9).

The BNM makes clear that the proposed policy document regulations do not apply directly to payment facilitators, as the BNM has specified the criteria of merchant acquirers that would be required to comply with the regulation. These include acquirers that are direct participants in a payment network providing merchant acquiring services (BNM 2021, 2.1), namely: "The criteria would cause third party acquirers/payment facilitators to be scoped out from the requirements in this policy document. Therefore, current third-party acquirers/payment facilitators will not be within the purview of FSA, although still allowed to conduct their business" (BNM 2020, 2). Importantly, though, the proposed regulations outline a variety of requirements for acquirers with respect to EPAIs. Malaysia's proposed regulations represent an example where service providers are considered an outsourced business.

United States

Two of the three US federal banking regulators—the Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency (OCC)—have specific sections in their examination manuals dedicated to merchant processing (FDIC 2007; OCC 2014). These manuals set out expectations for bank acquirers and bank examiners reviewing merchant processing activities. Though

BOX 2, *continued*

the manuals are fairly similar, the OCC's is more recent and addresses a wider variety of issues. Both manuals identify similar risks associated with merchant processing, including strategic risk, credit risk, operational or transaction risk, compliance risk, and reputational risk. The manuals also lay out key risk-management and control imperatives for acquirers. The referenced manuals do not include non-bank acquirers. Non-bank acquirers are addressed at the state level; an example, the American state of Georgia, is provided below.[35] The regulation of non-bank acquirers currently falls to the state financial regulators. However, the OCC has recently signaled that it would like to pursue a national "payments charter" that would likely cover non-bank acquirers. As with its proposed fintech charter, the move faces legal challenges from state regulators (Beyoud 2020).

At the federal level, two of the three banking regulators currently consider intermediaries under outsourcing regulation. If approved, the OCC's proposed payments charter would represent a more direct approach to intermediary regulation. Currently, some intermediaries, such as payment facilitators, are considered money services businesses by the state financial regulators and have to obtain licenses to operate in the states. PayPal and Square, for example, are licensed by most American state financial regulators.

India

The Reserve Bank of India (RBI) adopted standards on merchant sourcing and monitoring for commercial banks in 2011 that include merchant acquiring risk-management elements (RBI 2011a, 2011b). The standards were to be implemented by September 2012. In 2016, in an effort to "encourage banks to expand card acceptance infrastructure to a wider segment of merchants," the RBI emphasized that banks "may put in place their own Board approved policy on merchant acquisition" (RBI 2016, 1). In 2017 and 2020, the RBI began permitting cooperative banks (RBI 2017a) and regional rural banks (RBI 2020a) to serve as merchant acquirers. However, equivalent regulation is unavailable for non-bank acquirers. These measures were taken to further expand EPA to unserved merchant segments. The notices establishing these standards include risk-management requirements similar to those outlined by the RBI (2011a) for commercial banks. They also stipulate standards for financial soundness, including minimum capital and maximum nonperforming asset ratios for cooperative and regional reserve banks seeking to serve as acquirers.

The RBI merchant acquiring standards maintain that "wherever the activities are outsourced, the respective acquiring banks would still be responsible for ensuring adherence to the standards" (RBI 2011a, 38). This represents an outsourcing relationship. However, in 2020, the RBI issued specific regulations related to payment aggregators and payment gateways (RBI 2020b), representing a new direct approach to EPAI regulation.

Indonesia

Merchant acquirers are required to be licensed in Indonesia through Bank Indonesia's card-based payment instrument regulations (BI 2009a). Acquirers must demonstrate business feasibility and operational readiness. They must have a risk-management plan that outlines measures for mitigating liquidity risk, credit risk, operational risk, and reputation risk (BI 2009b). Additionally, acquirers need to have adequate security procedures in place for protecting data and authenticating the identity of customers. Further, Bank Indonesia's card regulations stipulate that the bank will supervise acquirers, focusing on risk management, regulatory compliance, and customer protection. The bank (2009a) defines an acquirer as a "Bank or Non-Bank Institution cooperating with merchant in the processing of data for card-based payment instruments issued by other parties" (BI 2009a, article 1.10, 5). Article 7 of the regulations (BI 2009a) makes clear that banks or non-banks can serve as acquirers, and both require a license.

American State of Georgia

In 2012, the American state of Georgia developed a specialized charter for merchant acquirer limited purpose banks (MALPBs) (Georgia General Assembly 2012). MALPBs "perform merchant acquiring activities or settlement activities" (Georgia General Assembly 2012, 7-9-2[4]). MALPBs must be chartered by the Georgia Department of Banking and Finance. The charter allows them to access payment card networks directly, without the sponsorship of another regulated financial institution, effectively enabling non-bank acquiring. The MALPB Act and the department's policy statement on MALPBs (GDBF 2014) set out of a variety of requirements for these entities. The MALPB charter discussed above applies to entities that would otherwise be considered non-banks. As with the other state banking regulators in the United States, the Georgia Department of Banking and Finance has regulatory jurisdiction, along with either the Federal Deposit Insurance Corporation

continued

BOX 2, *continued*

or the Federal Reserve, over commercial banks that are chartered in Georgia. Therefore, it would likely regulate commercial bank acquirers through its general-purpose bank regulatory standards. States generally have more direct regulatory jurisdiction over non-bank payment companies than federal regulators.

At the American state level, states may have some direct regulatory, or at least licensing jurisdiction, over certain EPAIs. This is applicable for the state of Georgia. For example, PayPal and Square are licensed by the Georgia Department of Banking and Finance.

European Union

The European Union's revised Payment Services Directive (PSD2) authorizes acquirers as payment institutions, and the rules are applied equally. Among other functions, the definition includes "acquiring of payment transactions," which "means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee" (EU 2015a, article 4[44]). The European Union indicates that the directive "introduces a neutral definition of acquiring of payment transactions in order to capture not only the traditional acquiring models structured around the use of payment cards, but also different business models, including those where more than one acquirer is involved" (EU 2015a, para. 10). It does not, however, address non-bank acquirers. PSD2 stipulates that "payment institutions" must be authorized and subject to capital requirements and safeguarding requirements, among other standards (EU 2015a, articles 7–10).

4.2 MANAGING THE RISKS OF ACQUIRER OUTSOURCING

Acquirers face barriers that can prevent them from achieving commercially viable economics and scale in efforts focused on financial inclusion. Outsourcing some functions can help them to address some of the following barriers: organizational inertia, which prevents alignment with segment needs; high costs, which prevent the achievement of viable business economics; and a lack of innovation focused on segment needs. In many markets, especially those with poorly developed acceptance footprints, the focus has been on business models and products that do not address the needs of small and medium-sized enterprises (SMEs), ill equipping many acquirers to serve this segment. Outsourcing provides an opportunity for merchant acquirers to quickly refocus on the growing SME opportunity—for example, through quick and agile deployment of necessary capabilities. Outsourcing provides an approach to deploy lower-cost business models and delivery approaches to reach SMEs quickly. Improved economics help to reach smaller merchants. Appropriate outsourcing arrangements are focused better on segment needs, equipping acquirers to reach SMEs with propositions that resonate. This may include, for example, products and associated processes, staffing models, agile systems, and distribution channels better aligned to the needs of the SME segment. Outsourcing partners may be younger, nimble firms, generally not burdened by legacy technology and processes.

In indirect regulation, there are two approaches to the regulation of acquirer outsourcing. A regulator can generally address outsourcing to EPAIs through general outsourcing regulations. Alternatively, a regulator can address acquirer outsourcing to EPAIs explicitly. This may include the stipulation of acquirer requirements specifically addressing the activities of EPAIs. Under both approaches, the responsibility for outsourced activities ultimately rests with acquirers.[36]

The scope of regulations addressing acquirers and their outsourced services to intermediaries varies across jurisdictions. Regulation in the United States, by focusing on the management of processor relationships, addresses a broad cross section of EPAIs, as does Malaysia, by addressing all outsourced parties. Egypt, on the other hand, specifically focus on payment facilitators, payment aggregators, and gateways. An explicit focus on EPAIs addresses several of the same issues tackled in direct regulation but with oversight responsibilities placed on the sponsoring bank or acquirer. Furthermore, the risks presented to bank and non-bank acquirers by outsourcing, and specifically by intermediaries, are similar. The difference between the two, however, is that non-bank acquirers cannot rely on a legacy bank regulation as a vehicle in mitigating these risks. In general treatments of outsourcing, it is common for regulators to point out the need for regulatory compliance by their partners with local laws and regulation (RBI 2006; CBK 2014; FSB 2020). For example, similar to PSD2, Kenya's national payment system regulations make clear

that PSPs cannot outsource core functions if the outsourcing arrangement would impair PSPs' internal controls or the Central Bank of Kenya's ability to supervise the PSP; furthermore, several authorities note the regulation of outsourcing should not be a hurdle for supervision.

Acquirers face strategic, legal, and compliance risks in outsourcing to EPAIs. Merchant acquisition encompasses several activities to identify, recruit, and contract with approved merchant prospects. An acquirer may not possess the appropriate staffing models, expertise, and associated processes to address the economic needs of MSMs. By outsourcing this function, some acquirers may be able to open up the MSM segment. One risk that may emerge is aligning the merchant mix onboarded by the intermediary with the portfolio and targeted market goals of the acquirer, identified as the strategic risk (FDIC 2014; OCC 2008). This also includes reputational risks that stem from the failure of an intermediary to perform its obligations properly. Another risk is ensuring that partners adhere to required processes, as the acquirer bares ultimate risk. The Bank for International Settlements' Joint Forum points out the need to address these risks in its guidelines on bank outsourcing (BCBS 2005). A regulator can mitigate such risks by developing clear policies for working with acceptance intermediaries and outsourcing in general (FSB 2020; RBI 2006). Furthermore, an acquirer can address many of these risks by incorporating provisions and obligations into its provider agreements.

Regulators may require due diligence by acquirers before they can enter into a contract with an intermediary. Risks identified during due diligence can be addressed through appropriate measures to control and manage risks, as well as on-going acquirer monitoring. These measures should ensure the adequacy of systems, staff capabilities, appropriateness of procedures, and roles of management and the board. At a high level, requirements can address due diligence and assessment reporting, such as risk assessments highlighted earlier in this section (BCBS 2005; RBI 2006; CBE 2019, article 6-1-5, 14). Another area of mitigation is intermediary monitoring reports. And yet, while "regulation through outsourcing" may rationalize monitoring, focusing the regulator on key players—the acquirer, in this case—it can concentrate risk and responsibility over such key players. Among other things, monitoring can include transaction monitoring of financial institutions to ensure compliance with agreed upon service-level agreements, charge-backs, consumer complaints, and submerchant monitoring, as well as suspicious activities, and incidents (CBE 2019, article 4-3, 12; FDIC 2014; OCC 2008; BNM 2020). Such reporting requires access to acquirer information and the ability to audit service providers (FDIC 2014; OCC 2008; BNM 2021).

Regulation through outsourcing may also misread reality, as outsourcers vary, and since the dimension of players might vary, or these operators may combine activities that might increase risk, reinforcing the need for due diligence, monitoring, and the ability to audit. The FDIC provides guidance that banks adopt board-approved payment processor approval programs that establish a bank acquirer's risk tolerance with respect to payment processors, verification approaches, and ongoing monitoring mechanisms. (See box 3.) These efforts may signal the need to implement an exit strategy. This is addressed in a later section on outsourcing contracts.

Regulators can seek to protect consumer data by highlighting existing requirements and the need for acquirers to comply with measures. One avenue for protecting consumer data is to require outsourcing providers to abide by bank standards regarding risk-management practices and information security policies regarding such information (CBE 2019, article 6-1-4, 14). This is a gap that may need to be addressed for non-bank acquirers. Another avenue is to provide outsourcers with guidance on the permissible use of customer data, given the importance of data in innovative new products and business models.[37] Finally, there is potential for outsourcing partners to outsource to fourth parties such data-sensitive activities as data storage.[38,39] This practice activity raises new risks around regulatory purview, regulator access, and the need for a regulator to possess the technical skills needed to assess such specialized fourth parties. One mechanism for addressing such risks is to require approval by the acquirer bank for intermediaries' outsourcing activities.

The protection of consumer funds can be addressed by requirements on both acquirers and EPAIs. Requirements can be tailored to the nature of acquirer control over settlement—namely, by the acquirer or through an intermediary settlement to the accounts of its submerchants. Regulators generally stipulate that acquirers are ultimately responsible for payment and settlement risk (BNM 2021), while specific requirements may differ depending on the services an intermediary provides (that is, provision of merchant acceptance or enablement of different payment types). Intermediaries, for example, might be required to settle funds within a specific time frame to submerchants' accounts, ensuring the predictability of cash flows. Regulators may also stipulate that an acquirer establishes a mechanism to ensure the complete control of settlement to submerchants based on the value of a predefined guarantee (CBE 2019, article 6-2-5, 15). Submerchant funds may be required to be segregated in a separate account, with the sponsoring acquirer (CBE 2019, article 6-2-16-4, 17).

Customer protection requires clear rules, a system for recourse, and an awareness of rights. In an indirect regulatory regime, the emphasis is on acquirer efforts to establish a risk policy addressing consumer protections (for example, refunds, fraud, and disputes). Clear rules are needed for settling disputes between the system users. The Egyptian regulator, for example, requires the sponsoring acquirer to establish clear rules for the resolution of disputes that may arise between the parties using the payment system, based on the delivery channel used. Malaysian regulators, on the other hand, require acquirers to ensure that their outsourcing partners have dispute-resolution mechanisms for merchants (BNM 2020). Regulators may also require that acquirers ensure that their intermediaries undertake activities to raise awareness among submerchants on how to exercise these rights, including how to use the system, extract required reports, and access data on specific transactions, and the

BOX 3

REGULATION OF OUTSOURCING TO EPAIs

This box illustrates several examples of regulating outsourcing to EPAIs. The examples focus on regulations tailored to EPAIs and address the cases of Egypt, the United States, and Malaysia.[40]

Egypt

The Central Bank of Egypt's (CBE) 2019 standard "Technical Payment Aggregators & Payment Facilitators Regulations" represents perhaps the clearest example of an indirect approach to EPAI regulation. The CBE stipulates several requirements for banks[41] vis-à-vis their acquirer relationships with intermediaries that are tailored to intermediary activities. The regulations apply to banks' relationships with payment facilitators and technical payment aggregators.[42]

The minimum standards lay out a wide range of requirements for banks. Above all, banks seeking to use technical payment aggregators or payment facilitators must obtain a license from the CBE to do so (CBE 2019, article 10). Further, banks must set out board-approved policies and strategies (CBE 2019, article 2) with respect to intermediary relationships that address, among other things, risk-analysis approaches, risk monitoring, control and mitigation, on-site inspection, due diligence, and risks related to refunds, fraud, disputes, and bankruptcy. The standards go on to lay out more specific considerations and expectations related to strategic risks, operational and transaction risks, compliance and legal risks, and reputational risks (CBE 2019, article 3). Further, they stipulate standards for anti-money-laundering/combating the financing of terrorism, suspicious activity reporting, and expectations for information-security policy (CBE 2019, articles 4 and 5). More broadly, the standards set a wide variety of "general rules for banks" using these intermediaries (CBE 2019, article 6).

United States

The United States represents another example of regulating acquirers' outsourced activities, with a focus on acceptance intermediaries. Specifically, the FDIC and OCC have issued guidance on managing payment processor relationships (FDIC 2014; OCC 2008). It is important to note that these agencies discuss payment processors in a broad sense, encompassing payment facilitators/aggregators and third-party payment processors. These guidance publications are complementary to the FDIC's and OCC's merchant processing examination manuals.

The FDIC guidance stresses that banks should **establish contracts** with payment processors that ensure their timely access to relevant information and their ability to close accounts or terminate contracts when necessary. The contracts should also stipulate ade-

Responsibility	Specific Imperatives
Due diligence and underwriting	Perform background checks of payment processors and merchants Verify that merchants are legitimate businesses Ensure that payment processors verify and review merchants
Ongoing monitoring	Ensure that payment processor provides information on merchants Monitor levels of unauthorized returns, charge-backs, and other suspicious activity Actively monitor consumer complaints against processors Conduct periodic audits of payment processors File suspicious activities reports and terminate relationships when necessary

continued

BOX 3, *continued*

quate reserve requirements for **charge-backs.** The FDIC guidance further requests that banks adopt board-approved payment **processor approval programs** that establish banks' risk tolerance with respect to payment processors, verification approaches, and ongoing monitoring mechanisms.

The FDIC and OCC guidance publications are similar, focusing on due diligence, underwriting, and ongoing monitoring of payment processors and their merchant clients. The guidance publications argue that these relationships often present heightened risks of various forms, due to the fact that banks—as acquirers operating with intermediaries—often will not have a direct relationship with merchants. Such risks include strategic risk, credit risk, operational or transaction risk, compliance risk, and reputational risk. The FDIC guidance also discusses the potential for heightened fraud risk, money-laundering risk, consumer protection risk, and legal risk. The table below catalogs selected risk-management and control responsibilities assigned to banks in their relationships with payment processors as outlined in the OCC's and FDIC's guidance

Malaysia

One of the pillars of Malaysia's proposed acquirer regulations (BNM 2021) is promoting the use of outsourcing arrangements. The proposed regulations address specific issues related to acquirer relationships with acceptance intermediaries, including payment facilitators and gateways. In addition, the proposed regulations specifically mention merchant recruitment agents and IT service providers. Key outsourcing imperatives for acquirers include the following:

- Maintaining **responsibility** for outsourced activities
- Ensuring that outsourcing partners verify that merchants are legitimate and not involved in fraudulent or illegal activities
- Ensuring that payment facilitator partners can handle **payment and settlement** risk and **settle transactions** for merchants in a timely manner
- Assuming responsibility for settlement when payment facilitators fail
- Conducting ongoing **monitoring and periodic audits** of outsourcing partners, including the periodic monitoring of submerchant transactions
- Ensuring that outsourcing partners have dispute-resolution mechanisms for merchants
- Conducting **due diligence** of outsourcing partners, including the assessment of their financial viability and risk-management capacity. In addition, assessing the extent of the concentration of risk with respect to a single provider and mitigations measures.
- Establishing detailed **outsourcing agreements** with service provide. Furthermore, subcontracting by the service provider will not dilute its accountability.

ability to raise and research objections as well as document such transactions (CBE 2019, articles 6-2-12 and 6-2-13, 16). In sum, a regulator can strengthen consumer protections by mandating the establishment of customer protection policies, rules, and associated processes. Some regulators mandate the acquirers and service providers to send reports to keep them abreast of complaints as well as incidents.

Outsourcing of operations and IT can expose an acquirer to financial loss. These risks stem from fraud, refunds, and disputes; defects in the work-system; and service unavailability, cyberattacks, and so on. In an indirect regulatory approach, regulators can compel acquirers to take several actions to mitigate these risks. As noted at the beginning of the section, some of these may explicitly address EPAIs but with responsibility placed on the sponsoring acquirer. Acquirers can be required to ensure that their information security policy is updated regularly and that it appropriately addresses electronic payments, including monitoring policies, measures, and controls, individual responsibility, and execution mechanisms and measures (CBE 2019, article 5-1, 13). In addressing outsourcing in general, the guidelines of the Basel Committee on Banking Supervision point to the need for contingency plans (BCBS 2005), while others note the need to address continuity (FSB 2020). Finally, the Basel committee's guidelines also point out the need to address issues around IT, such as data and cybersecurity (BCBS 2005).

Financial risk is inherent in outsourcing. A critical financial risk is the potential need for a sponsoring acquirer to shut down an outsourcer. This need could arise due to insolvency or investment losses, among other causes. This risk can be mitigated by monitoring an outsourcing provider's financial status, annual reports, and cash-flow reports; implementing reserve requirements, if applicable; and adopting an exit strategy, such as transferring the business to another third-party provider. The Malay-

sian regulator, for example, requires a registered sponsoring acquirer to assume responsibility for settlement to a merchant should a payment facilitator fail (BNM 2021). US regulators put forth the need for enhanced due diligence and monitoring to address outsourcing risks as well as the need for reserve requirements, if applicable, to address charge-backs (FDIC 2014; OCC 2008).

Other outsourcing risks include concentration and cross-border risks. Outsourcing activities can potentially be concentrated with a single provider, or several activities might be outsourced to a single provider, creating concentration risk and potentially leading to systemic risk in the case of the operational or financial failure of an outsourcing provider with significant market power (BCBS 2005). A regulator or acquirer might lack the purview, physical access, or capability to address outsourced activities (BCBS 2005; CBK 2014).[43] This is particularly problematic when the outsourcing provider is located outside the bank's jurisdiction.[44]

BOX 4

INDIRECT REGULATION OF GENERAL ACQUIRER OUTSOURCING

This box focuses on the more general treatment of outsourcing. The review encompasses guidelines for outsourcing from the Bank for International Settlement and a consultative document from the Financial Stability Board (FSB). Two cases are presented, addressing general acquirer outsourcing in India and Kenya.

Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision's Joint Forum issued outsourcing guidelines for financial services firms and regulators in 2005.[45] The Joint Forum defines outsourcing as a "regulated entity's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future" (BCBS 2005, 4). At the time the guidelines were issued, IT and administrative functions were the most frequently outsourced areas, but financial activities and others were increasingly being outsourced.

The Joint Forum's primary concern revolved around the outsourcing of core functions and the potential to transfer risk, management, and compliance to unregulated entities. According to the Joint Forum, a wide variety of potential risks are associated with outsourcing, including strategic, reputation, compliance, operational, exit-strategy, counterparty, country, contractual, access, concentration, and systemic risks (BCBS 2005, 11–12). The Joint Forum lays out nine guiding principles related to outsourcing, which deal with outsourcing policies, risk management, core functions, due diligence, contracts, contingency plans, confidentiality, regulators' assessment of outsourcing, and regulators' risk awareness. The Joint Forum summarizes key actions financial institutions can take as follows: "draw up comprehensive and clear outsourcing policies, establish effective risk-management programs, require contingency planning by the outsourcing firm, negotiate appropriate outsourcing contracts, and analyze the financial and infrastructure resources of the service provider" (BCBS 2005, 2).

Financial Stability Board

The FSB issued a more recent consultative document in 2020 that discusses the regulatory and supervisory landscape with respect to outsourcing and third-party risk management (FSB 2020). The document is based on the results of a survey of supervisors in member countries. As a discussion paper that contains a request for comment, this document could serve as a baseline for future standards in this area.

The FSB explains that outsourcing has become more common and more complex. Similar to the findings of the Basel Committee on Banking Supervision (2005), outsourcing in the area of information and communications technology (ICT) is still the most prevalent type, especially as financial institutions increase their reliance of cloud-based services. Importantly, the FSB speculates that the COVID-19 pandemic has likely deepened reliance on outsourcing. All respondents to the FSB survey have outsourcing standards in place. The survey further reveals a universal regulatory theme: that outsourcing does not absolve management from liability for third parties' activities. Other key areas in outsourcing standards involve risk management, business continuity and exit strategies, cybersecurity, data protection, and operational resilience, among other areas. Some standards give regulators direct supervisory access to third parties. Despite some cases of direct access to third parties, all responding authorities generally rely on the regulated entity to manage the outsourcing risks themselves. In general, the FSB emphasizes that outsourcing contracts should not interfere with regulated entities' compliance obligations.

The FSB also flags several areas of emerging concern. First, supervisors face practical challenges to oversee-

continued

BOX 4, *continued*

ing outsourcing arrangements, including resource constraints, access limitations, and increasingly complex supply chains. On this final point, though some supervisors spell out standards related to third parties' subcontractors, authority is often on shaky ground in this area. Further, supply chains are becoming increasingly deep, with fifth- and sixth-level outsourcing arrangements. Second, cross-border arrangements are common and pose regulatory challenges. Finally, concentration and systemic risk in the outsourcing space is an increasing concern.

Country Cases

India

The RBI (Reserve Bank of India) has been active in regulating outsourcing. In 2006, it released its "Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks" (RBI 2006). The guidelines incorporate the outsourcing guidelines of the Bank for International Settlements' Joint Forum (BCBS 2005). Recently, in August 2021, the RBI issued "Framework for Outsourcing of Payment and Settlement-Related Activities by PSOs" (RBI 2021). The RBI guidelines make clear that outsourcing does not absolve management of liability for outsourcing functions. Further, they insist that outsourcing cannot interfere with regulatory compliance. In general, the RBI maintains that the "underlying principles for these guidelines are that the regulated entity should ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers and RBI nor impede effective supervision by RBI" (RBI 2021).

More specifically, the guidelines address a wide variety of outsourcing expectations related to the following:

- Risk management, including the needs to establish an outsourcing policy and to evaluate, monitor, and control the myriad risks posed by outsourcing, such as strategic, reputation, compliance, operational, legal, exit-strategy, counterparty, country, contractual, and concentration and system risks
- Due diligence
- Outsourcing contracts
- Confidentiality and security
- Business continuity
- Monitoring outsourced activities
- Handling complaints with respect to outsourced activities
- Reporting suspicious activity

The RBI has released a number of follow-up standards since the 2006 guidelines. First, in 2015, the RBI was compelled to issue a circular emphasizing that the 2006 standards apply to the area of subcontracting, after observing increased noncompliance with the guidelines in the area of subcontracting (RBI 2015). Further, in 2017, the RBI released outsourcing standards for non-bank financial companies (RBI 2017b). The content of the 2017 standards is very similar to that of the 2006 guidelines. Recently, the RBI released "Framework for Outsourcing of Payment and Settlement-related activities by PSOs" (RBI 2021) and guidelines on the regulation of both payment aggregators and gateways (RBI 2020b). The release of these guidelines has moved the RBI to a direct regulatory approach of EPAIs detailed in chapter 3.

Kenya

In addition to specific standards for the retail agents of payment service providers (PSPs), the Central Bank of Kenya's National Payment System Regulations (NPSR) spell out requirements for PSPs seeking to outsource operational functions (CBK 2014). The central bank strongly emphasizes that outsourcing arrangements should not impair PSPs' compliance with the NPSR. In particular, the NPSR make clear that PSPs cannot outsource core functions if the outsourcing arrangement would impair PSPs' internal controls or the bank's ability to supervise the PSP. Further, the Central Bank of Kenya requires outsourcing contracts to grant it supervisory access to the third party (CBK 2014, 23: 5a).

The central bank clarifies that it considers an outsourced function to be "material" if it interferes with regulatory compliance, impairs financial performance, or harms the "soundness or the continuity" of payment services (CBK 2014, 23: 4). Further, the NPSR make clear that management is liable for the activities of the third party.

4.3 AUTHORIZATION OF ACQUIRER OUTSOURCING

In the indirect approach, regulators authorize acquirers to work with outsourcing partners, which can include EPAIs. The regulator will typically have no role in assessing or performing due diligence on intermediaries. Instead, acquirers will be required to perform these activities before their partners can provide their services on the market. These requirements, while similar to some of those outlined in the chapter on direct regulation, differ in focus, putting the onus on the acquirer, rather than the intermediary. It is the acquirer that makes the decision to work with an outsourcing partner such as an EPAI, and it is this entity that bears ultimate responsibility for their partners.[46,47]

Some regulators might require acquirers seeking to outsource services to EPAIs to obtain an approval or authorization from the supervisory authority, while other regulators may just request a notification by the acquirer or stipulate the need for other actions by acquirers that outsource activities. To obtain consent, an acquirer could detail its plans for engaging an EPAI, addressing, for example, its market-development objectives, provision of compliance reporting, and proposal for system inspections by the regulator. In addition, an acquirer's board of directors may be responsible for ratifying a work strategy developed by its senior management.

To address financial and operational concerns, an acquirer might be required to conduct due diligence on the financial and operational capabilities of an intermediary prior to entering into an agreement. The CBE, BNM, FDIC, and OCC underscore the responsibility of the acquirer to conduct due diligence on intermediaries, while the Basel Committee on Banking Supervision notes the need for an acquirer to perform due diligence on potential outsourcing partners.[48] Furthermore, acquirers may need to ensure that their plan to use the intermediary's services aligns with their strategic direction (CBE 2019, article 2-1, 9; FDIC 2014; OCC 2008; BNM 2021). In governance, a bank can detail the responsibilities of its provider's board and senior management. Regulators tend to request the acquirer to perform continuous auditing and risk monitoring of the intermediary's activities.

Prudential requirements are generally applicable to nonbank acquirers. Regulators may require minimum capital requirements to ensure financial soundness. The FDIC and OCC, two of the three US financial regulators, have specific sections in their examination manuals dedicated to merchant processing (FDIC 2007; OCC 2014).[49] Both manuals acknowledge that regulatory capital rules do not specifically address merchant processing, but banks should nevertheless hold appropriate capital for merchant processing, including higher levels of capital for riskier merchant processing activities. The manuals stress that regulators have flexible authority to require banks to hold more capital associated with these activities. Both manuals point out that card scheme rules generally stipulate limits related to processing volumes relative to capital, but regulators may set stricter limits for higher-risk activities, including for high-risk merchant categories and excessive charge-backs, among other reasons.

Regulators can establish additional controls on outsourcing providers. One control directed at EPAIs is to place limits on the size of submerchants' annual electronic turnover. While scheme rules impose limits, regulators can impose stricter limits—indirectly on EPAIs through their sponsoring bank—better suited for market conditions, if they feel these to be warranted. Another area is to prohibit intermediaries from contracting with risky merchant categories (for example, pyramid marketing, jewelry sales, lottery shops, crypto currency, and crowd funding) (CBE 2019, article 6-2-14, 17). Some regulators may allow facilitators and gateways to acquire unregistered merchants, while other regulators may require intermediaries to verify the legal standing of submerchants.[50] This may have the effect of preventing many MSMs from being able to offer electronic acceptance services.

Regulators may stipulate that outsourcing contracts address specific concerns. Insertion of explicit clauses and terms into contracts can explicitly address several of the risks that regulators seek to mitigate. Malaysia requires the establishment of detailed outsourcing agreements. The Kenyan regulator requires outsourcing contracts to grant the Central Bank of Kenya supervisory access to the third party (CBK 2014, 23, 5a). In the United States, the FDIC guidance stresses that banks should establish contracts with payment processors that ensure their timely access to relevant information and their ability to close accounts or terminate contracts when necessary, effectively using a contract to define an exit strategy. Exit strategies might include measures to ensure the continuity of the service by addressing its transferability to another third party and continuation-of-security clauses even after the contract termination.[51]

5. Regulating Payment Schemes

This chapter focuses on the regulation of payment schemes by examining their characteristics, rules, and interaction with EPAIs. A scheme establishes the rules, standards, and requirements and provides the coordination that enables the electronic transfer of value through a payment instrument between its members. Businesses such as EPAIs become scheme members by meeting scheme-imposed obligations and standards. Through membership and associated scheme rules, EPAIs and other entities play a well-defined role across the payment value chain to support the electronic transfer of value through a scheme payment instrument. To understand the legal environment in which schemes operate and set their rules, the paper takes a step back to examine cases of scheme regulation that set the context for the role of schemes and their interaction with EPAIs. This context is useful in understanding the role of a scheme in rule making, licensing EPAIs, and schemes' interactions with EPAIs.

The chapter is organized as follows: The first section describes card schemes and their key elements and touches on mobile-money schemes. It highlights efforts to regulate card payment schemes in general, as well as efforts to regulate card pricing. The second section characterizes scheme management, addressing issues of relevance to EPAIs. The third section focuses on authorization and oversight considerations for EPAIs working within payment schemes.

5.1 OVERVIEW OF PAYMENT SCHEMES

Payment schemes, with their associated rules and standards, govern how PSPs may become scheme members as well as use scheme products and their networks to execute payments. This section examines two types of payment schemes: card schemes and mobile-money schemes. A ***payment scheme*** is a set of rules and associated arrangements, functions, and procedures that enable the holder of a payment instrument to effect a payment or cash-withdrawal transaction with a party other than the issuer of the payment instrument. This enables schemes to organize and manage the activities supporting electronic payments. ***A payment system is the set of instruments, procedures, and rules for the transfer of funds between or among participants.*** The system includes the participants and the entity operating the arrangement, according to the CPMI (CPMI 2016). The payment system includes the infrastructure that processes payment transactions executed through a payment instrument in line with the rules defined by the system operator. There are several types of payment systems, including electronic as well as paper-based systems, such as checks. ***Schemes rules enable the exchange of value between members.*** Scheme rules govern critical dimensions of electronic payments that enable the exchange of value between members. An EPAI, for example, by becom-

ing a scheme member, can facilitate the acceptance of transactions through a scheme-branded payment instrument (for example, card or direct debit) issued by that scheme's members. The EPAI's acceptance activities are governed by the scheme's rules, agreed to by the EPAI when it became a scheme member. Furthermore, the EPAI will have agreed to specific terms by entering into a contractual agreement with a scheme-registered merchant acquirer, including scheme-mandated provisions such as submerchant obligations, the need to comply with scheme rules, and entering into an agreement with each submerchant (McCarty 2012). The combination of these elements enables payment services to be offered in a predictable manner to achieve the benefits afforded by a payment network.

Regulators have typically focused their efforts on payment system operators, the system rules, and the actors that participate in these systems. Authorities in some cases regulate the payment scheme as a payment system, taking into consideration the system operations. This chapter focuses on payment schemes that provide the general framework where specific rules for intermediaries exist. However, any reference to a scheme could be applicable to the payment system as long as the system maintains similar rules of coverage.

Two Types of Retail Payment Schemes

Schemes support standardization and predictability. Card schemes that are managed by the international and domestic card schemes have been dominated by four-party models and focused on person-to-merchant payments. Mobile-money schemes have been dominated by three-party models and person-to-person payments, and many of them enable merchant acceptance. What these schemes have in common are their efforts to create an enabling environment that is standardized, including standards for messages, application programming interfaces, security, complaint management, and so on, to promote efficient payments. The mechanisms for achieving this differ and are related in some ways to the scheme's history, level of development, and the nature of interoperability that is enabled between scheme members.

A card scheme has established rules that address payment instruments, each with its own rules, under the same brand. Card schemes use either a three- or four-party model to manage their payments business. Scheme capabilities are supported by an interbank switch that may or may not be operated by the scheme. A scheme has more control in a three-party model, while it is easier to build a larger acceptance footprint through a four-party model because of the greater ease of building a network effect. Scheme rules specific to a PSP enable the provider to execute transactions through a payment card. These rules and associated standards govern membership, assure equal and predictable treatment, and, finally, enable integration into the scheme network, to ensure the efficient execution of payment transactions.

Mobile-money schemes are different from card schemes. A rich landscape has emerged in mobile payments since mobile-money operators entered the fray around 2008, when they realized customers could save their money and transact through them without the need for a bank account. Mobile-money schemes could either follow a three-party model—where the customer and merchant are clients of the same mobile-money service provider, such as Alipay, PayTM, and OrangeMoney—or be organized under a four-party model, where the customer and merchant are clients of two different mobile-money service providers that are connected through an interoperability platform, such as Mowali. The GSMA identified several characteristics for mobile-money scheme: (1) the ability of customers to participate in the scheme without having a bank account (unless required by the regulator); (2) the ability of customers to access and withdraw funds easily using an extensive agent network; and (3) the ability of customers to use the service through simple devices, which do not necessarily need to be smart devices.[52] Mobile-money schemes for the most part have remained in their own closed ecosystems. Nevertheless, under such three-party arrangements, the scheme operator may outsource merchant acceptance to other entities. Mobile-money scheme rules often cover the settlement process, dispute resolution, customer support, and training.

As mobile-money schemes develop, there are several paths to expanded interoperability. The GSMA has detailed several technical options that mobile-money providers may consider to achieve interoperability between themselves. Examples include both domestic and global hubs as technical models for enabling interoperability between participants. One example of such a deployment is provided by the announcement by Orange Group and MTN Group of Mowali (Mobile Wallet Interoperability) in November 2018 of a joint venture hosting interoperability services for domestic and international mobile-money transactions. Mowali is built on the open-source platform Mojaloop (GSMA 2020a), which, in turn, provides a scheme model to support real-time transactions between mobile-money providers. It offers flexibility to customize a number of scheme dimensions regarding ownership, participation, the scope of rules, and applicable use cases, among others.[53] In addition to Mowali's hub-based model, other examples of interoperable schemes exist in Ghana, also a hub-based model; Uganda, an aggregator model; and Tanzania and Madagascar, which are based on bilateral arrangements (GSMA 2020b). Mobile-money interoperability is able to

support a large number of use cases, including person to person, person to business, person to application, person to government, application to person, business to person, and government to person, among others. The responsibility for managing agents or merchant aggregators is typically assigned to mobile-money service providers

Many mobile-money service providers offer a merchant-specific platform that allows merchants to receive payments from customers and pay bills, suppliers, and employees. Typically, providers equip merchants with a special SIM card for this purpose. In many cases, this platform is provided by a third party with which the mobile-money provider contracts. Mobile-to-mobile payments are the most common manner of payments, but providers are working on more seamless solutions (McCarty 2012). Traditional mobile-to-mobile payments are cumbersome, because payers need to enter payment amounts and the merchant's account number. Recent developments, such as merchant-initiated QR payment and request to pay, embed merchant payment information in the QR code, facilitating the payment process.

Mobile-money schemes may rely on bilateral contractual agreements and other commercial agreements. Some of these schemes have emerging merchant acceptance (for example, the case of M-Pesa in part as a result of its relationship with Kopo Kopo). A short terms-and-conditions document, which accompanies merchant agreements, is the closest structure akin to payment card scheme rules (Safaricom 2014, d). Some notable clauses make clear that Safaricom bears no liability for errors, such as underpayment and incorrect entry of merchant numbers (Safaricom 2014, 8.5.2). The terms and conditions do state that the merchant shall conduct reversals when there is clearly a payment error (Safaricom 2014, 5.1). The terms and conditions also spell out some of Safaricom's obligations, including settlement, providing customer service, and secure website access. Safaricom establishes detailed know-your-customer requirements for merchants (Safaricom 2019).

5.2 REGULATING CARD PAYMENT SCHEMES

Payment schemes, unlike payment system operators, have not been regulated in a systematic manner. In those cases where schemes have been regulated, regulators have focused on discrete aspects, such as promoting competition (EU 2015a), promoting access rules (RBA 2004a, 2004b), efforts to encourage self-regulation (HKMA 2016), scheme registration (BSP 2019), and scheme licensing (BOT 2018a, 2018c), as well as the regulation of interchange fees, which is addressed in detail in box 5. Direct regulation of payment systems and payment system operators, on the other hand, has been more systematic. In many jurisdictions, the payment system regulations are implicitly applicable to payment schemes. In such cases, the regulators focus both on the operations of the payment system and on all issues related to system rules.

Payment Card Fee Regulation

While schemes have not been regulated systematically, it sometimes happens that authorities regulate rates of interchange fees or merchant discounts. National authorities have begun to shift their focus from litigation to regulation in recent years (Hayashi and Maniff 2014). Table 7 catalogs practices for regulating payment card fees in

TABLE 7: Payment Card Fee Regulations in Selected Economies

Jurisdiction	Standard
Australia	The weighted average interchange fee benchmark for credit card transactions is 0.5 percent, and the ceiling for any individual transaction is of 0.8 percent (RBA 2016a). The weighted average interchange fee benchmark for debit cards is $A 0.08, with a ceiling of $A 0.15, or 0.2 percent, for any individual transaction (RBA 2016b).
Brazil	Debit card interchange fees are capped at 0.8 percent for any given transaction, and the weighted average fee is 0.5 percent (Ayres and Mandl 2018; Hayashi and Maniff 2020).
China	Interchange fees are capped at 0.35 percent for debit cards and 0.45 percent for credit cards (Hayashi and Maniff 2020).
India	For small merchants, ***merchant discount rates*** for debit card transactions are capped at 0.4 percent for physical point-of-sale infrastructure, including online transactions, and at 0.3 percent for QR code–based acceptance. For all other merchants, ***debit card merchant discount*** rates are capped at 0.9 percent and 0.8 percent for the separate infrastructure categories, respectively (RBI 2017).{-2017a -OR- 2017b?-}
European Union	Interchange fees are capped at 0.3 percent and 0.2 percent for card-present credit and debit card transactions, respectively (EU 2015b). They are generally capped at 1.5 percent and 1.15 percent for card-not-present credit and debit card transactions, respectively (EU 2019).
South Africa	Interchange fees vary between 0.36 percent and 0.53 percent for debit cards and between 1.41 percent and 1.89 percent for credit cards, based on whether transactions are card-present or card-not-present and whether issuers and acquirers are EMV or 3D Secure compliant (SARB 2014).
United States	The Federal Reserve sets an interchange fee cap for debit card issuers at $0.21 plus 5 basis points of the transaction's value (Federal Reserve 2011, 43420). Issuers with less than $10 billion in assets are exempt from the rule.

BOX 5

REGULATORY FRAMEWORKS FOR CARD PAYMENT SCHEMES

This box provides an overview of several frameworks used by regulators to address card payment schemes. The frameworks highlight a range of experiences.

Australia

The Reserve Bank of Australia has designated Mastercard (credit, debit, and prepaid), Visa (credit, debit, and prepaid), American Express companion cards, and EFTPOS (narrow definition) as "payment systems." Designated payment systems may be subject to rules, such as access regimes and interchange-fee regulations. The reserve bank has established access regimes only for Mastercard and Visa credit card schemes (RBA 2004a, 2004b). The access regimes entail some basic criteria related to applying to participate in the schemes, such as eligibility, assessment of applications, transparency, and certification and reporting. Scheme administrators must certify that participants meet risk-related eligibility and assessment criteria annually, but the standards are not prescriptive about the types of risk-management criteria that should be evaluated.

European Union

In addition to setting interchange fees for credit and debit cards at 0.3 percent and 0.2 percent, respectively, the European Union's Interchange Fee Regulation (EU 2015b) sets various fee-related transparency standards that schemes must follow. Importantly, it also requires independence between card schemes and processing entities (EU 2015b, A7.1a) and prohibits bundling scheme and processing fees (EU 2015b, A7.1b). These separation standards are intended to increase competition in the processing market by allowing independent processors to compete for schemes' customers (EU 2015b, [33]).

Hong Kong

Hong Kong's "Code of Practice for Payment Card Scheme Operators" (HKMA 2016) is a code of conduct designed by and applicable to the scheme operators and is endorsed by the Honk Kong Monetary Authority. Thus, it is a "self-regulation" approach for the schemes. It is not a legally binding regulation; rather, the monetary authority works with scheme operators to ensure compliance with the code.

The code outlines a range of safety, efficiency, transparency, and monitoring expectations for schemes. These include establishing clear scheme rules and procedures, ensuring operational reliability and business continuity, risk management, fraud monitoring and awareness, due diligence for outsourcing arrangements, and data security, among many other standards. Most of the standards related to four-party schemes are framed within the context of "encouraging" their acquirers and issuers to adhere to the code.

Philippines

Payment card schemes are considered operators of payment systems and must be registered by the Bangko Sentral ng Pilipinas (BSP 2019). The registration requirements are not significant. Visa and Mastercard are registered as operators of payment systems by the central bank (BSP 2021).

Pakistan

The State Bank of Pakistan's Rules for Payment System Operators and Payment Service Providers (SBP 2014) describe payment system operators and PSPs as entities "engaged in operating and/or providing Payment Systems related services like electronic payment gateway, payment scheme, clearing house, ATM Switch, POS Gateway, E-Commerce Gateway etc. acting as an intermediary for multilateral routing, switching and processing of payment transactions" (SBP 2014, 3). To the extent that card schemes are considered payment system operators in Pakistan, they would be subject to a variety of standards, including minimum capital, operational, risk-management, security, confidentiality, dispute-resolution, and reporting requirements, among others.

Thailand

Payment card networks are considered "designated payment systems" in Thailand, according to the Payment System Act (Kingdom of Thailand 2017). Payment card networks must be licensed, according to the Bank of Thailand (2018a). Many networks are licensed as "payment card network services" in Thailand, including American Express, JCB International, Mastercard, UnionPay, Visa, Thai Payment Network, and National ITMX. Further, the bank (2018b) lays out financial, governance, risk-management, security, system-user-protection, efficiency, and competitiveness standards for designated payment systems. It is important to note that these regulations exist in addition to Thailand's separate regulations governing both merchant acquirers and EPAIs. Indeed, Thailand takes a direct approach to regulating intermediaries, acquirers, and schemes.

selected large markets across the globe. While most of regulators addressed the rates of interchange fees among issuer and acquirer banks, the RBI focused on the merchant discount rate.

Card Scheme Components

Six principal components underpin a payment card scheme. These are governance arrangements, contracts, payment instruments, scheme rules, clearing and settlement rules, and complaints and dispute management. These components govern members and ensure the standardization necessary to execute electronic payments through a payment instrument. The standardization, predictability, and coordination provided by these components allow new members to join the scheme and enable transactions between the customers of other scheme members.

Governance by the scheme of its members is executed through rules and requirements established by the scheme. These rules govern most aspects of card issuing, authorization, clearing, and acquiring. They can be general, regulating such criteria as network membership, brand standards, technical and acceptance standards, settlement procedures, and standards for arbitrating disputes. They can also be more specific, governing the relationship between the scheme and its members as well as their agents—for example, the admission of new members into the scheme. Scheme rules have been augmented in recent years to address the membership of EPAIs, such as payment facilitators and their obligations. In addition to managing rules, schemes enforce the rules and may impose assessments on members that fail to comply.

In establishing contractual relationships with members, schemes impose obligations to promote the smooth and predictable functioning of the scheme. Contracts are established under the auspices of the rules and set conditions for PSPs, including requirements on the use of the scheme's marks, processes, and operational infrastructure, among others. Other details stipulated within an EPAI contract might include obligations for scheme participation as well as rights for contract termination. The obligations included in contracts will depend on the functional role of an organization in the scheme. For example, contractual obligations will differ between acquirers, payment facilitators, payment gateways, and merchants. Furthermore, there are required terms that must be included in merchant agreements (Mastercard 2020, section 5.1.2, 95).

Schemes have established rules and develop new rules in response to the evolving nature of payments—for example, to address the evolution of acceptance and the emergence in the acceptance value chain of new intermediaries, such as payment facilitators. These rules address the responsibilities and obligations of actors across the acceptance value chain and establish pricing through interchange.

The rules laid out by a scheme detail the execution of payment transactions through a specific payment instrument. A scheme may support several payment instruments, and its rules may be unique to that particular instrument (for example, debit card, credit card, or mobile wallet).

Schemes have established rules for clearing and settlement. These rules are extended to EPAIs in defining their obligations and rights for settlement. Mastercard, for example, notes that acquirers may permit payment facilitators to access settlement funds for the purpose of paying submerchants in accordance with the terms of their submerchant agreements (Mastercard 2020, section 7.6.5, 109, 156). The schemes provide additional requirements regarding settlement, such as the timing obligations for crediting a merchant account.[55]

Finally, scheme rules put forth standards for addressing complaints and resolving disputes. Schemes establish standards and guidelines to address complaints and disputes arising for a number of reasons, including addressing charge-backs or disputed transactions. Such rules establish clear, transparent, and predictable arbitration processes.

5.3. ELEMENTS OF CARD SCHEME MANAGEMENT AND REGULATION

This section touches on key elements of scheme rules that interact with EPAIs along critical regulatory dimensions and, more specifically, areas that help promote the efficient functioning of schemes and minimize risk, akin to the mandate of regulators. Given this similarity in objectives, there is a parallel focus between regulators and the card schemes with their well-developed rules.

Card Scheme Governance

Rules, standards, and other requirements are the mechanisms by which a scheme governs its relationships with its members. At the member level, scheme rules govern the relationship between a scheme and its members, as well as between the scheme and the members' agents. The responsibility for developing, implementing, and enforcing these rules and associated requirements

resides with the payment scheme. The establishment of a scheme-governing body and representation of customers and merchants on the scheme-governing body depends on the nature of scheme ownership. All participants in a scheme are subject to and bound by the scheme's charter documents and its rules.

Schemes undertake direct monitoring to identify and gauge risks and mandate members to undertake certain activities. Scheme rules, for example, stipulate that they may audit and review a member to ensure compliance with scheme rules and standards[56] These rules encompass EPAIs and their outsourced providers. While schemes members are required to comply with applicable laws on anti-money-laundering and combating the financing of terrorism, they also maintain anti-money-laundering programs.[57] Visa states that its program is designed within the context of regulations applicable to schemes to prevent the schemes' systems from being used to facilitate money laundering and the financing of terrorist activities (Visa 2020, section 10.1.3, 554). Scheme rules also stipulate the need for members to monitor their agents. Acquirers, for example, are required to monitor payment facilitators with whom they have contracted for acceptance services.[58] Other examples include acquirer-monitoring programs and merchant fraud monitoring.[59]

Card Scheme Rules and Party Liability

Card scheme rules define the parameters for participation by PSPs and their associated liabilities. Rules lay out the roles and obligations for organizations, such as EPAIs, that become scheme members. Scheme rules touch on a broad range of themes, including branding, risk management, clearing, and settlement. For example, clearing and settlement is of concern, because it may give rise to default or insolvency of the service provider. In particular, a PSP acting as acquirer might face liquidity or credit risk if an issuer is unable to settle an obligation (ECB 2019, 8). Schemes publish rules and additional guidelines as necessary.[60] Furthermore, scheme rules lay out the unique roles of members, such as issuers and acquirers. Both major international schemes address payment facilitators.

The obligations and liabilities of different types of members are detailed by card scheme rules. Rules addressing acquirers, for example, require them to monitor their payment facilitators for compliance with scheme rules. Put differently, acquirers possess and are required to exercise "supervisory powers" over EPAIs. Furthermore, acquirers are responsible for the acts of payment facilitators, as payment facilitators sign merchant acceptance agreements on behalf of acquirers. Obligations placed directly upon EPAIs include necessary due diligence in onboarding merchants and the need to include required language in merchant agreements. The rules issued by international major schemes furthermore specify that an acquirer bears the ultimate liability for acceptance. Schemes reserve several rights for themselves, to ensure the integrity of the payment system they manage, including the ability to apply fees for noncompliance[61] and the right to terminate merchant agreements, among others.[62] The latter enables them to intervene directly and address risks stemming from EPAIs.

Merchant onboarding illustrates an EPAI's scheme obligations. Scheme rules stipulate that, before contracting with a prospective merchant, a payment facilitator must perform a due diligence review of the prospective merchant candidate considered adequate by the scheme. This includes a site visit, if applicable, to the business premises or a suitable alternative. Upon successful completion of onboarding requirements and before doing business with a merchant, a payment facilitator needs to execute a merchant agreement that contains clauses requiring merchants to comply with scheme rules and obligations.[63] This may require merchants to comply with applicable laws and regulations and comply with scheme rules, and include the right of the scheme to terminate the payment facilitator's agreement with a sponsored merchant.[64]

Card schemes have actively addressed clearing and settlement. Schemes have stipulated rules to address settlement by payment facilitators. Namely, a payment facilitator must pay its submerchants for all transactions it has submitted on their behalf. This obligation is not fulfilled until a submerchant has received payment, notwithstanding any payment arrangements. Furthermore, submerchant agreements provide a vehicle for addressing charge-back reserves to be held back by the facilitator.

Competition and Market Structure

Card schemes have established clear guidelines for the participation of payment service intermediaries. These guidelines delineate requirements, obligations, and standards to which PSPs must adhere. Yet it should be noted that schemes generally rely on the acquirer members to monitor payment facilitators. While in the case of acceptance, scheme rules apply to members and include specific provisions on monitoring payment facilitators, acquirers remain responsible for the acts of payment facilitators, as payment facilitators sign merchant acceptance agreements on behalf of acquirers. Furthermore, additional requirements are placed on acquirers that enroll payment facilitators. In the case of EPAIs, they are required first to become registered with a scheme; then they may enter into a contract with a scheme mem-

ber, such as an acquirer, to start enrolling merchants. To become a registered payment facilitator, an applicant needs to be financially sound. In the case of Visa, this requires a minimum equity of $100 million. Visa's rules state that this amount may be waived in exchange for assurances and evidence of risk controls and other requirements.[65] Among other things, such requirements may include the sponsoring acquirer attesting to a due diligence review of the payment facilitator with which it wants to contract.[66]

A payment facilitator must enter into a merchant agreement with each of its sponsored merchants to formalize their arrangements. At this point, there are obligations and requirements that must be met regarding the merchants with which the payment facilitator seeks to do business.[67] Schemes can impose fees and noncompliance assessments on payment facilitators that do not meet its rules and standards.[68] Other rules include the need for payment facilitators to meet several operational and processing requirements, such as the assignment and use of merchant identifiers and other critical information.

Operational and IT Security Risks

Card scheme rules address operational and IT security risks that can affect their payment networks. These efforts focus on operational risks, the continuity of operations, and the security of data, both stored data and data in motion, as addressed through cybersecurity standards and programs, such as PCI. These cybersecurity standards and programs are relevant to all customers, merchants, and service providers, such as EPAIs, that store, process, or transmit account, card, cardholder, or transaction data (Mastercard 2021, chapter 2).

Financial Risks

Schemes address several types of financial risks, through both their rules and the requirements they impose on intermediaries to become members. One critical financial risk presented by merchants to EPAIs is their solvency and the associated risk that they may be unable to meet their obligations. Such obligations may arise from customer charge-back or prepaid customer goods or services, among others. Schemes require mechanisms in merchant agreements by EPAIs to address such risks—namely, by allowing merchant agreements to give payment facilitators the ability to withhold amounts for charge-back reserves or similar purposes in accordance with scheme standards.[69, 70] Another potential area of risk that schemes could address is general business risk. In Mexico, for example, the Mexican regulators put requirements on PSPs when moving into adjacent businesses.[71]

A third area of financial risk addressed is intermediary payments to those accepting cards. Scheme rules provide for payment to the payment facilitator on behalf of a sponsored merchant, noting that the payment facilitator needs to credit the sponsored merchants account promptly after the deposit of funds.[72] Scheme rules, unlike rules issued by regulators, don't go as far as to require segregated accounts to prevent the comingling of merchant funds with those of an acceptance intermediary.

Time limits for crediting a beneficiary account are addressed by scheme rules. Scheme rules provide guidance on acquirer funding of payment facilitator accounts and, in turn, by payment facilitators to submerchants. Visa rules, for example, extend this to provide explicit timing guidelines for Brazil.[73]

Consumer and Data Protection

Schemes seek to protect consumers and data. This protection is important for the integrity of payment systems and for the consumer confidence and trust necessary to support their active use. Schemes have put limitations on the disclosure of transaction information.[74] Both international schemes, for example, do not allow their members to convey or disclose personal or proprietary data without express permission.[75] Furthermore, rules have been developed to address data sharing to support open banking. The requirements include the need for intermediaries to ensure compliance with local laws, provide appropriate notice to customers of their intended processing of personal information, and adopt appropriate security measures around the storage and processing of personal data, among others.[76]

5.4 AUTHORIZATION AND LICENSING CONSIDERATIONS FOR EPAIS

There are similarities in the objectives of both scheme and regulator efforts to register members and authorize EPAIs. To reiterate a point made earlier, both are motivated to promote efficient networks and minimize risk. The major differences between them is the profit motivation of schemes and the broader focus of the regulator.

Regulators have not licensed or authorized international schemes systematically. Nevertheless, there are cases where domestic schemes have received authorization from the local regulator. This is the case in the Philippines, with the requirement for scheme registrations (BSP 2019), and the requirement for scheme licensing in Thailand

(BOT 2018a, 2018b). Some regulators designate domestic or international schemes as systemically[77] or prominently[78] important payment systems and, hence, require a sort of authorization and regular monitoring.

Card schemes typically authorize intermediaries to operate as members through their registration, while acquirers are responsible of monitoring the contracted EPAIs, and specifically facilitators. International schemes generally require registration, while domestic schemes are sometimes reluctant to authorize domestic intermediaries. Registration requirements include criteria for network membership, such as financial strength, competent management, and the need to comply with scheme requirements and obligations. Once registered as a scheme member, an intermediary is subject to scheme requirements. These include the need for EPAIs to enter into provider agreements with merchants for activities to facilitate electronic payments through payment cards.

In regulating domestic or international schemes, regulators, after reviewing scheme rules, may apply changes. Scheme or system rules function as the governing body, addressing most aspects of acquiring, card issuing, authorization, and clearing. Regulators may impose changes that affect some of the applicable rules. This is especially true of submerchant volume limits established by international schemes on payment facilitators. For example, while Visa applies a limit of $100,000 on the annual transaction volume of a submerchant working through a payment facilitator,[79] some regulators may apply amendments to increase or decrease this limit. Finally, regulators may request transparency in the application of fees and may intervene to address applied fees for interchange or merchant discount rates. Schemes may adjust their rules at a regional or country level to be consistent with local laws or regulations. For example, Mastercard adjusted its rules on data protection as they apply to its European region to align with developments in the regulation of open banking and the introduction of new PSPs in that region.[80]

Schemes use contracts to expand definitions of the obligations of EPAI members. These obligations are imposed through their acquirer agreements and their submerchant agreements. In addition to the obligations associated with becoming members of a scheme, EPAIs sign an agreement with a merchant acquirer to provide acceptance services on behalf of that acquirer. Under this relationship, the scheme is clear that the acquirer is ultimately responsible and, hence, must take actions to ensure the proper behavior by the EPAI. Under this agreement, however, the payment facilitator agrees to comply with scheme rules and is responsible for cardholder disputes and customer service issues that may arise among others. In addition to acquirer agreements, EPAIs must enter into merchant agreements with each of their submerchants.

6. Conclusion

An approach to financial inclusion grounded in payments holds tremendous promise. Among other things, digital payments reduce direct costs for banks and service providers and reduce transaction costs, such as time, for users. EPA has huge potential to harness networks effects and economies of scope in the provision of an expanded array of valuable services, improving access to different sectors of the economy. Crucial to the success of a payments-centered financial-inclusion program is the need for a robust acceptance footprint that is aligned with the payment behaviors of the target population for inclusion. More than 180 million MSMs are estimated to be in the developing countries, most of which don't accept electronic payments. EPA would not only extend to this huge merchant sector but also cover the 4.5 billion customers who regularly transact with them daily.

Merchant acquirers, the traditional vehicle for developing payment acceptance, lag in their efforts to build out acceptance for underserved and unbanked populations. EPAIs, on the other hand, address several barriers preventing the expansion of payment acceptance by acquirers to those merchants and businesses frequented by the underbanked and the unbanked. First, they are nimble and quick to align to segment needs, overcoming inertia by acquirers. Second, intermediaries incorporate innovative technology into their products and solutions. And finally, they are quick to deploy new and lower-cost business models to reach SMEs. Yet the introduction of EPAIs into the acceptance value chain extends a number of existing risks and introduces new considerations. A key rationale for regulating EPAIs is to achieve balance between the benefits of greater inclusion and the risks introduced by EPAIs—or to put it differently, to achieve policy objectives, such as facilitating the extension of financial services to excluded populations in a manner that balances the risks of doing so.

This paper has highlighted and elaborated on these risks, which include, among others, financial risks, such as the liquidity of intermediaries; risk to consumers, in the form of unauthorized transactions and disputes; risks to consumer—merchants—funds and data through unauthorized access; and the risks to IT and operations, with impacts to their safety and the continuity of operations. Addressing and mitigating these risks can maintain and build trust in electronic payments—a foundational requirement for end-user engagement and usage—promoting the viability of systems serving the underserved and unbanked.

The paper encourages regulators to take a proactive leadership role in understanding the risks of EPAIs to develop the appropriate balance of regulations. Some regulators may choose not to intervene in the affairs

of intermediaries. Still others may choose to regulate them directly, while others may address intermediaries through regulations focused on acquirer outsourcing—focused generally on outsourcing or explicitly focused on EPAIs. Some regulators may choose to focus on the regulation of schemes. Finally, regulators may choose to employ elements of several approaches at the same time. For a number of reasons, regulators may pursue different approaches to the regulation of EPAIs. These reasons may include their regulatory capabilities, current regulatory approach, and development, as well as market characteristics, such as the level of development, among others.

Various approaches being undertaken by regulators have been highlighted in this paper. It has not sought to opine on the efficacy or appropriateness of the approaches discussed, but to lay out the topography of the landscape, so that others may benefit from an understanding of efforts that have been undertaken. In so doing, it provides those facing the same issues both insights and some direction for moving forward.

The direct regulation approach applies when the regulator issues regulations that address EPAIs directly. Regulations will typically be directed at specific types of intermediaries or can target certain functions, regardless of the type of intermediary. Upon issuing direct regulations, the authorities will expect any entity providing or anticipating providing such services to apply for a license or authorization from the regulator. This approach addresses intermediaries directly by specifying the necessary conditions for providing a specific service.

When the regulation of intermediaries occurs indirectly, through acquirers and their outsourced services, the activities of EPAIs are seen as the responsibility of the acquirer, and these activities are considered to be outsourced by the acquirer to a third party. The regulator may issue regulations that are specific to the acquiring business. The regulator could decide to address specific types of intermediaries as special types of outsourcing, specifying certain requirements for those intermediaries. Alternatively, the regulator could issue regulations that address the requirements for outsourcing services in general. The approach chosen for licensing or authorizing intermediaries may differ from one authority to the other. Nevertheless, the acquirer is ultimately liable for the deeds of its intermediaries.

The third approach addresses the whole payment scheme with all its participants, including intermediaries. Regulators may choose to ensure that the scheme governing body or system operator manages all risks within the scheme, including the risks presented by EPAIs. Part of the rationale is that EPAIs are part of a payment scheme or system, such as a card scheme or mobile-payment scheme. As such, scheme or system rules will include the conditions for intermediary service delivery. With this approach, regulators could apply certain conditions—either general or specific—to intermediaries based on their type. Nevertheless, it would be the responsibility of the scheme governing body or the direct participant of the scheme (acquirers) to ensure EPAIs' compliance with the regulations. Under this approach, intermediaries would not necessarily need to be licensed by the authorities but would need to be authorized by the scheme governing body or system operator.

GENERAL NOTES ABOUT THE APPLICATION OF THE REGULATORY APPROACHES

While applying one or more of the previous approaches, the authorities may consider the legal, regulatory, and supervisory environment and the scope of authorities. We reiterate several issues that have been raised earlier about the implementation of these approaches within different jurisdictions.

The scope of regulations, oversight, and supervision could vary from one jurisdiction to the other based on legislative structure. For example, some authorities may designate intermediaries as service providers under the supervision and oversight of the central bank. In other jurisdictions, non-bank financial institutions could be under the supervision of a different authority. Such distinctions may be relevant within the central bank itself. Within some central banks, the oversight and supervision functions for the PSPs, including intermediaries, are performed by the payment system oversight unit. In others, the supervision of non-bank financial institutions is performed through the supervision unit.

Besides payment systems safety and efficiency, financial consumer protection and data protection could be the objectives of some central banks. However, in some jurisdictions, the responsibility for these objectives may be assigned to institutions other than the central bank. The oversight unit within some central banks may have a specific mandate for protecting the customers of the payment systems or users of payment instruments. Alternatively, the mandate could be assigned to different authorities in other jurisdictions. The same might be true for a financial data-protection mandate. Central banks should be vigilant about issuing regulations out of their legal mandate and ensure that the scope and objectives of their regulations are within the central bank mandate.

The burden of each approach on regulatory resources should be considered. In some cases, regulatory resources may be constrained. In such circumstances, consideration should be given to the resource requirements of a particular regulatory approach. For example, some authorities might prefer the direct regulation approach, as it allows the authorities to monitor the risks of EPAIs closely. However, this approach might increase the burden on the central bank. Other approaches may put more responsibility on the regulated financial institutions acting as acquirers, as opposed to the regulator, in overseeing or monitoring the activities of intermediaries. The regulator may be able to rely on the skills and capabilities of the regulated financial institutions to oversee the intermediary effectively. In addition to freeing up the regulator's scarce resources, there are other potential advantages to the regulator, such as the ability to leverage the business acumen of their commercial banks. However, this approach might increase risks, as some financial institutions are not well equipped to monitor and oversee the activities of the intermediaries. Having one intermediary outsourced by multiple financial institutions could increase the oversight burden on this intermediary. In this specific case, concentration risk might be seen by neither the monitoring entities nor the central bank.

The regulator should consider a functional approach, instead of an institutional approach, where the requirements are associated with risks of a specific function or business. In a functional approach, requirements would be consistent for banks and non-banks to avoid regulatory arbitrage. In applying this approach, regulators should be very clear about the separation of different products provided by the same service provider. For example, an entity that provides payment gateway and facilitation services might be subject to the regulations associated with each of those services. The same applies for an entity that could provide switching services and third-party processing of card management or ATM terminal processing. In doing so, the overseer or supervisor should be sensitive to the supervisory burden on the supervised entities and ensure harmonization of activities.

The regulator should encourage innovation and the introduction of new business models. Innovative models typically address gaps in the market structure. The emergence of EPAIs in many jurisdictions can fill the gap where typical acquirers can't reach to MSMs due to the business models applied by these acquirers. EPAIs cooperate with acquirers to extend the reach of acceptance services. The financial authorities should realize the market's need for such players and issue regulations that encourage entrepreneurs to innovate such models. The regulator should avoid restrictive requirements that might discourage new players, such as high capital or operational requirements. The regulator should enhance the market competitiveness through having a level playing field for all players.

Finally, the level of market sophistication and structure could be an important factor in the selection of the regulatory approach. A market with few dominant providers might require the central bank to take a direct regulatory approach. A market characterized by many nondominant providers might be better suited to an indirect regulatory approach. Having strong and mature payment schemes or system operators with detailed rules and clear operational requirements would allow the central bank to apply the existing scheme rules while appending the rules with country-specific conditions.

References

AFI (Alliance for Financial Inclusion). 2018. *Fintech for Financial Inclusion: A Framework for Digital Financial Transformation*. AFI, September 2018.

Arkwright. 2020. *Managing Merchant Credit Risk: Post Covid 19 Acquiring and Acceptance*. May 20, 2020.

Ayres, Marcela, and Carolina Mandl. 2018. "Brazil Caps Debit Card Fees, May Limit Them Further." Reuters, March 26, 2018. https://www.reuters.com/article/us-brazil-cenbank-regulation/brazil-caps-debit-card-fees-may-limit-them-further-idUSKBN1H22XL.

BCBS (Basel Committee on Banking Supervision). 2005. *The Joint Forum: Outsourcing in Financial Services*. BIS, February 2005. https://www.bis.org/publ/joint12.pdf.

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

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

Beyoud, Lydia. 2020. "Payments Shaping Up as Next Turf Battle between OCC, States." Bloomberg Law, July 17, 2020. https://news.bloomberglaw.com/banking-law/payments-shaping-up-as-next-turf-battle-between-occ-states.

BI (Bank Indonesia). 2009a. Bank Indonesia Regulation Number: 11/11/PBI/2009 Concerning Management of Card-Based Payment Instrument Activities. https://www.bi.go.id/en/publikasi/peraturan/Documents/PBI%20Nomor%2011.11.PBI.2009%20tentang%20APMK%2031%20Maret%202009.pdf.

BI (Bank Indonesia). 2009b. "Management of Card-Based Payment Instrument Activities." Circular Letter No. 11/10/DASP. https://www.bi.go.id/en/publikasi/peraturan/Documents/SE%20Nomor%2011.10.DASP%20tentang%20APMK.pdf.

BI (Bank Indonesia). 2016. Regulation No. 18/40/PBI/2016 Concerning Payment Transaction Processes. https://www.bi.go.id/id/publikasi/peraturan/Pages/pbi_184016.aspx#.

BIS (Bank for International Settlements). 2019. *The Design of Digital Financial Infrastructure: Lessons from India*. BIS Paper No. 106. BIS, December 2019.

BNM (Bank Negara Malaysia). 2020. *Merchant Acquiring Services*. Exposure Draft BNM/RH/ED 032-5. July 17, 2020. https://www.bnm.gov.my/documents/20124/943361/Merchant+Acquiring+Services+-+Exposure+Draft.pdf/4aed917a-4ad1-5cab-400b-a1e0e3996341?t=1600348844368.

BNM (Bank Negara Malaysia). 2021. *Merchant Acquiring Services*. BNM/RH/PD 028-119, September 15, 2021.

BOG (Bank of Ghana). 2019. *Guideline on Operations of Electronic Payment Channels in Ghana*. https://www.bog.gov.gh/wp-content/uploads/2019/08/Guidelines-on-Operations-of-Electronic-Payment-Channels-in-Ghana.pdf.

BOG (Bank of Ghana). 2020. "License Categories & Permissible Activities." https://www.bog.gov.gh/wp-content/uploads/2020/07/License-Categories-with-Secretarys-comments_2.pdf.

Bossone, Biagio, and Massimo Cirasino. 2001. The Oversight of the Payments Systems: A *Framework for the Development and Governance of Payment Systems in Emerging Economies*. Payment and Securities Clearance and Settlement Systems Research Series No. 1. CEMLA and World Bank, July 2001.

BOT (Bank of Thailand). 2018a. Regulations on General Supervision of Undertaking Designated Payment Service Business. April 2018. https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610082.pdf.

BOT (Bank of Thailand). 2018b. Regulations on Supervision of the Designated Payment Systems Business. April. https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610087.pdf.

BOT (Bank of Thailand). 2018c. Regulations, Procedures and Conditions on Application for License and Registration to Undertake Designated Payment Services Business. April 2018. https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610088.pdf.

BOT (Bank of Thailand). 2018d. Regulations, Procedures, and Conditions on Application for License to Undertake Designated Payment Systems Business. April. https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610086.pdf.

BOT (Bank of Thailand). 2018e. Stipulation on Designated Payment Services. https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610195.pdf

BSP (Bangko Sentral ng Pilipinas). 2019. "Rules and Regulations on the Registration of Operators of Payment Systems." Office of the Governor Circular No. 1049. September 2019. https://www.bsp.gov.ph/Regulations/Issuances/2019/c1049.pdf.

BSP (Bangko Sentral ng Pilipinas). 2021. "List of OPS with Certificate of Registration (COR)." March. https://www.bsp.gov.ph/PaymentAndSettlement/COR.pdf.

CBE (Central Bank of Egypt). 2019. Technical Payment Aggregators & Payment Facilitators Regulations. https://www.cbe.org.eg/_layouts/download.aspx?SourceUrl=%2Fen%2FPaymentSystems%2FRegulationsDL%2FTechnical%20Payment%20Aggregators%20%26%20Payment%20Facilitators%20Regulations.pdf.

CBK (Central Bank of Kenya). 2014. The National Payment System Regulations, 2014. https://www.centralbank.go.ke/wp-content/uploads/2018/12/NPSRegulationsNew2014-1.pdf.

CBN (Central Bank of Nigeria). 2018a. Regulatory Requirements for Non-Bank Merchant Acquiring in Nigeria. Exposure Draft PSM/DIR/GEN/CIR/01/003. September 7, 2018. https://www.cbn.gov.ng/Out/2018/BPSD/Exposure%20Draft%20of%20Regulatory%20Requirementsfor%20NonBank%20Merchant%20Acquiring%20in%20Nigeria.pdf.

CBN (Central Bank of Nigeria). 2018b. "Circular on the Exposure Draft of New CBN Licensing Regime (License Tiering) for Payment System Providers." BPS/DIR/GEN/CIR/05/012. October 15, 2018. https://www.cbn.gov.ng/Out/2018/PSMD/Circular%20on%20the%20exposure%20draft%20of%20new%20CBN%20licensing%20regime%20(Licence%20tiering)%20for%20payment%20system%20providers%20.pdf.

CBN (Central Bank of Nigeria). 2020a. Guidelines on Operations of Electronic Payment Channels in Nigeria. June 2020. https://www.cbn.gov.ng/Out/2020/CCD/Reviewed%20and%20Approved%20Guidelines%20on%20Operations%20of%20Electronic%20Payment%20Channels%20in%20Nigeria%202020.pdf.

CBN (Central Bank of Nigeria). 2020b. "New License Categorisations for the Nigerian Payment System." Circular PSM/CIR/GEN/CIR/01/22. December 9, 2020.

CBN (Central Bank of Nigeria). 2021. Regulatory Framework for Non-Bank Acquiring in Nigeria. May 2021.

Chamber of Deputies of the Congress of the Union (*Cámara de Diputados del H. Congreso de la Unión*). 2018. Mexican Fintech Law (*Ley para Regular las Instituciones de Tecnología Financeria*), March 9, 2018.

Chang, Howard, David S. Evans, and Daniel D. Garcia Swartz. 2005. "The Effect of Regulatory Intervention in Two-Sided Markets: An Assessment of Interchange-Fee Capping in Australia." *Review of Network Economics* 4, No. 4 (December): 328–58.

CPMI (Committee on Payments and Market Infrastructures). 2014. *Non-Banks in Retail Payments*. September 2014. https://www.bis.org/cpmi/publ/d118.pdf.

CPMI (Committee on Payments and Market Infrastructures). 2016. "Glossary" (web page). https://www.bis.org/cpmi/publ/d00b.htm.

CPSS (Committee on Payment and Settlement Systems). 2003. *A Glossary of Terms Used in Payments and Settlement Systems*. BIS, March 2003. https://www.bis.org/cpmi/glossary_030301.pdf.

CPSS (Committee on Payment and Settlement Systems). 2012. *Innovations in Retail Payments*. BIS, May 2012. https://www.bis.org/cpmi/publ/d102.pdf.

CSBS (Conference of State Bank Supervisors). 2014. *Third Party Payment Processors Job Aid*. February 2004, rev. August 2014. https://www.csbs.org/system/files/2017-11/Third_Party_Payment_Processor_Job_Aid%20revised%20Aug14.pdf.

Daly, Jim. 2020. "Merchants Bracing for Higher Reserve Requirements from Acquirers." Digital Transactions, June 8, 2020. https://www.digitaltransactions.net/merchants-bracing-for-higher-reserve-requirements-from-acquirers/.

Dodd-Frank Wall Street Reform and Consumer Protection Act. Pub. L. No. 111-203, 124 Stat. 1376 (2010). https://www.govinfo.gov/content/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf.

D'Silva, Derryl, Zuzana Filková, Frank Packer, and Siddharth Tiwari. 2019. *The Design of Digital Financial Infrastructure: Lessons from India*. BIS Paper No. 106. BIS, December 2019.

Durbin, Dick. 2010. "Durbin Statement on His Debit Card Swipe Fee Amendment." Press release, May 13, 2010. https://www.durbin.senate.gov/newsroom/press-releases/durbin-statement-on-his-debit-card-swipe-fee-amendment.

EBA (European Banking Authority). 2017. Final Report on the EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the Information to Be Provided for the Authorisation of Payment Institutions and E-Money Institutions and for the Registration of Account Information Service Providers. EBA/GL/2017/09, November 7, 2017. https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2.

EBA (European Banking Authority). 2019. *Final Report on EBA Guidelines on Outsourcing Arrangements*. EBA/GL/2019/02. February 25, 2019. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1.

EC (European Commission). 2016. "Antitrust: Regulation on Interchange Fees." Memo, June 9, 2016. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2162.

EC (European Commission). 2019. "Antitrust: Commission Accepts Commitments by Mastercard and Visa to Cut Inter-Regional Interchange Fees." Press release, April 29,

2019. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2311.

ECB (European Central Bank). 2019. *Card Payments in Europe—Current Landscape and Future Prospects: A Eurosystem Perspective*. ECB, April 2019. https://www.ecb.europa.eu/pub/pdf/other/ecb.cardpaymentsineu_currentlandscapeandfutureprospects201904~30d4de2fc4.en.pdf.

EcoCash. 2020a. "Merchants" (web page). https://www.ecocash.co.zw/about/merchants.

Edgar, Dunn & Company. 2020. *Interchange Fee Regulation Impact Assessment Study*. January 2020.

EU (European Union). 2007. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007L0064.

EU (European Union). 2015a. Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.

EU (European Union). 2015b. Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on Interchange Fees for Card-Based Payment Transactions. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex-%3A32015R0751.

EU (European Union). 2019. Summary of Commission Decision of 29 April 2019 Relating to a Proceeding under Article 101 of the Treaty on the Functioning of the European Union and Article 53 of the EEA Agreement.

EY and CE (Copenhagen Economics). 2020. *Study on the Application of the Interchange Fee Regulation*. European Commission, 2020.

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

{-DELETE COMMENT?- Not sure what is it – You may keep it for further internal processing }See FIGI Innovation Paper and check FATF references in Mexico Section

FCA (Financial Conduct Authority). 2019a. *Payment Services Regulations and Electronic Money—Our Approach*. June 2019. https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.

FCA (Financial Conduct Authority). 2019b. "Payment Services Regulations 2017 and Electronic Money Regulations 2011." September 2019. https://www.fca.org.uk/firms/payment-services-regulations-e-money-regulations.

FCA (Financial Conduct Authority). 2021a. *Payment Services and Electronic Money—Our Approach: The FCS's Role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011*. November 2021 (version 5). https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.

FCA (Financial Conduct Authority). 2021b. "Payment Services Regulations 2017 and Electronic Money Regulations 2011," (web page). https://www.fca.org.uk/firms/payment-services-regulations-e-money-regulations.

FDIC (Federal Deposit Insurance Corporation). 2007. "Merchant Processing," chapter 19 in *Risk Management Examination Manual for Credit Card Activities*. https://www.fdic.gov/regulations/examinations/credit_card/pdf_version/ch19.pdf.

Federal Reserve System. 2011. Debit Card Interchange Fees and Routing, Final Rule. *Federal Register* 76, No. 139 (July 20, 2011). https://www.govinfo.gov/content/pkg/FR-2011-07-20/pdf/2011-16861.pdf.

FDIC (Federal Deposit Insurance Corporation). 2014. "Guidance on Payment Processor Relationships." Financial Institution Letters. https://www.fdic.gov/news/financial-institution-letters/2008/fil08127a.html.

FFIEC (Federal Financial Institutions Examination Council). 2014. "Third-Party Payment Processors—Overview." BSA/AML Manual. https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/11.

FSB (Financial Stability Board). 2020. *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*. Discussion Paper, November 9, 2020. https://www.fsb.org/wp-content/uploads/P091120.pdf.

GDBF (Georgia Department of Banking and Finance). 2014. Merchant Acquirer Limited Purpose Banks. https://dbf.georgia.gov/sites/dbf.georgia.gov/files/related_files/document/MALPB-PolicyStatement.pdf.

Georgia General Assembly. 2012. Georgia Merchant Acquirer Limited Purpose Bank Act. https://www.legis.ga.gov/legislation/35642.

Government of Australia. 2012. "E-Commerce: Payment Gateways." https://web.archive.org/web/20121118194457/http://www.digitalbusiness.gov.au/online-payments-and-donations-benefits-of-e-commerce/e-commerce-payment-gateways/.

Govil, Sameer. 2016. *Perspectives on Accelerating Global Payment Acceptance*. Visa. https://usa.visa.com/dam/VCOM/download/visa-everywhere/global-impact/perspectives-on-accelerating-global-payment-acceptance.pdf.

GSMA. 2020a. *The Many Paths to Mobile Money Interoperability: Selecting the Right Technical Model for Your Market*. GSMA, June 2020. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/06/GSMA_Many-paths-to-mobile-money-interoperability-2.pdf.

GSMA. 2020b. *Tracking the Journey towards Mobile Money Interoperability: Emerging Evidence from Six Markets: Tanzania, Pakistan, Madagascar, Ghana, Jordan and Uganda*. GSMA, June 2020. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/06/GSMA_Tracking-the-journey-towards-mobile-money-interoperability-1.pdf.

Hayashi, Fumiko, and Jesse Leigh Maniff. 2014. "Interchange Fees and Network Rules: A Shift from Antitrust Litigation to Regulatory Measures in Various Countries." *Payment System Research Briefing*, October 2014. Federal Reserve Bank of Kansas City.

Hayashi, Fumiko, and Jesse Leigh Maniff. 2020. "Public Authority Involvement in Payment Card Markets: Various Countries—August 2020 Update." Federal Reserve Bank of Kansas City. https://www.kansascityfed.org/~/media/files/publicat/psr/dataset/pub-auth_payments_var_countries_august2020.pdf.

HKMA (Hong Kong Monetary Authority). 2016. Code of Practice for Payment Card Scheme Operators. September. https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Payment_card.pdf.

Johnson, Jamie. 2019. "What Is a Payment Aggregator?" CO by US Chamber of Commerce. https://www.uschamber.com/co/run/finance/payment-aggregator-explained.

Katakam, Arunjay. 2014. *Setting Up Shop: Strategies for Building Effective Merchant Payment Networks*. GSMA, October 2014. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/10/2014_DI_Setting-up-shop_Strategies-for-building-effective-merchant-payment-networks.pdf.

Khiaonarong, Tanai, and Terry Goh. 2020. *Fintech and Payments Regulation: Analytical Framework*. IMF Working Paper WP/20/75, May 2020.

Kingdom of Thailand. 2017. Payment System Act. October 16, 2017. https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/SiteAssets/Law_E40_Payment.pdf.

Kingdom of Thailand. 2018. Stipulation on Designated Payment Services. Ministry of Finance. April 17, 2018. https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610195.pdf.

Lopez, Mariana. 2020. *Mobile Money: Driving Formalisation and Building the Resilience of MSMEs*. GSMA, June 2020. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/06/Mobile-Money-Driving-formalisation-and-building-the-resilience-of-MSMEs.pdf.

MAS (Monetary Authority of Singapore). 2020a. *A Guide to the Essential Aspects of the Payment Services Act 2019*. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Payment-Service-Providers/Guide-to-the-Payment-Services-Act-2019.pdf?la=en&hash=B03712F4EEEE907C39BA2C-12DE63A545495EE1C2.

MAS (Monetary Authority of Singapore). 2020b. *Frequently Asked Questions (FAQs) on the Payment Services Act (PS Act)*. April 13, 2020. https://www.mas.gov.sg/-/media/MAS/Fintech/Payment-Services-Act/Payment-Services-Act-FAQ-13-April-2020.pdf.

Mastercard. 2001. *Submission to Reserve Bank of Australia, June 8, 2001 (as revised July 20, 2001)*. https://www.rba.gov.au/payments-and-infrastructure/credit-cards/iii-submissions-vol2/o1-mastercard-final.pdf.

Mastercard. 2016. "Submission to the RBA Review of Card Payments Regulation." February 3, 2016. https://www.rba.gov.au/payments-and-infrastructure/submissions/standards-for-card-payments-systems/pdf/mastercard.pdf.

Mastercard. 2017. *Building Electronic Payment Acceptance at the Base of the Pyramid to Advance Financial Inclusion*. Mastercard, October 2017.

Mastercard. 2019. Mastercard Rules. December 19. https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-rules.pdf.

Mastercard. 2020. Mastercard Switch Rules. December 8, 2020. https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-switch-rules-manual.pdf.

Mastercard. 2021. Mastercard Rules. September 28, 2021. https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-rules.pdf.

McCarty, M. Yasmina. 2012. *eWallet Merchant Payments: GSMA Discussion Paper*. GSMA, October 2012. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_eWallet-Merchant-Payments.pdf.

Miller, Phillip M., and Daniel G. Salazar. 2013. *Expanding Card Acceptance to Small Merchants Globally through Mobile Point of Sale (MPOS)*. MasterCard Advisors, May 2013. https://mpos.mastercard.com/corporate/_assets/img/features/mpos_white_paper_final_0507.pdf.

Mukharlyamov, Vladimir, and Natasha Sarin. 2019. *The Impact of the Durbin Amendment on Banks, Merchants, and Consumers*. Faculty Scholarship at Penn Law.

Nautiyal, Anant, Bart-Jan Pors, and Bruno Martins. 2020. *QR Code Merchant Payments: A Growth Opportunity for Mobile Money Providers*. GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/08/QR-Code-Merchant-Payments-A-growth-opportunity-for-mobile-money-providers-incl-full-appendices.pdf.

OCC (Office of the Comptroller of the Currency). 2008. "Payment Processors: Risk Management Guidance." OCC Bulletin 2008-12, April 24, 2008. https://www.occ.treas.gov/news-issuances/bulletins/2008/bulletin-2008-12.html.

OCC (Office of the Comptroller of the Currency). 2014. *Merchant Processing.* Version 1.0, August 2014. Booklet in *Comptroller's Handbook*. https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/merchant-processing/pub-ch-merchant-processing.pdf.

Pasti, Francesco, and Anant Nautiyal. 2019. *Mobile Money for Enterprise Customers: Addressing the Financial Services Needs of MSMEs in Sub-Saharan Africa*. GSMA, February 2019. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/GSMA-Mobile-Money-for-Enterprise-Customers.pdf.

Peek, Sean. 2020. "A Complete Guide to Payment Gateways." CO by US Chamber of Commerce. https://www.uschamber.com/co/run/finance/payment-gateways-for-business.

RBA (Reserve Bank of Australia). 2002. *Reform of Credit Card Schemes in Australia IV: Final Reforms and Regulations Impact Statement*. August 2002. https://www.rba.gov.au/payments-and-infrastructure/credit-cards/final-reforms/complete-stmt.pdf.

RBA (Reserve Bank of Australia). 2003. *Payments System Board Annual Report 2003*. https://www.rba.gov.au/publications/annual-reports/psb/2003/pdf/2003-psb-ann-report.pdf.

RBA (Reserve Bank of Australia). 2004a. Access Regime for the MasterCard Credit Card System. https://www.rba.gov.au/media-releases/2014/pdf/mr-14-22-gazette-notice-mastercard.pdf.

RBA (Reserve Bank of Australia). 2004b. Access Regime for the Visa Credit Card System. https://www.rba.gov.au/media-releases/2014/pdf/mr-14-22-gazette-notice-visa.pdf.

RBA (Reserve Bank of Australia). 2016a. The Setting of Interchange Fees in the Designated Credit Card Schemes and Net Payments to Issuers. Standard No. 1 of 2016. https://www.rba.gov.au/payments-and-infrastructure/review-of-card-payments-regulation/pdf/standard-no-1-of-2016-credit-card-interchange-2017-11-20.pdf.

RBA (Reserve Bank of Australia). 2016b. The Setting of Interchange Fees in the Designated Debit and Prepaid Card Schemes and Net Payments to Issuers. Standard No. 2 of 2016. https://www.rba.gov.au/payments-and-infrastructure/review-of-card-payments-regulation/pdf/standard-no-2-of-2016-debit-and-prepaid-card-interchange-2017-11-20.pdf.

RBA (Reserve Bank of Australia). 2016c. Scheme Rules Relating to Merchant Pricing for Credit, Debit and Prepaid Card Transactions. Standard No. 3 of 2016. https://www.rba.gov.au/

payments-and-infrastructure/review-of-card-payments-regulation/pdf/standard-no-3-of-2016-scheme-rules-relating-to-merchant-pricing-2016-05-26.pdf.

RBA (Reserve Bank of Australia). 2016d. *Review of Card Payments Regulation*. Conclusions Paper. May 2016. https://www.rba.gov.au/payments-and-infrastructure/review-of-card-payments-regulation/pdf/review-of-card-payments-regulation-conclusions-paper-2016-05.pdf.

RBA (Reserve Bank of Australia) and ACCC (Australian Competition and Consumer Commission). 2000. *Debit and Credit Card Schemes in Australia: A Study of Interchange Fees and Access*. October 2000. https://www.rba.gov.au/payments-and-infrastructure/resources/publications/payments-au/interchg-fees-study.pdf.

RBI (Reserve Bank of India). 2006. Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks. RBI/2006/167. November 3, 2006. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.PDF.

RBI (Reserve Bank of India). 2009. Directions for Opening and Operation of Accounts and Settlement of Payments for Electronic Payment Transactions Involving Intermediaries. RBI/2009-10231, November 24, 2009.

RBI (Reserve Bank of India). 2011a. *Working Group on Securing Card Present Transactions: Report and Recommendations*. May 31, 2011. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/SCP020611FS.pdf.

RBI (Reserve Bank of India). 2011b. Security Issues and Risk Mitigation Measures Related to Card Present (CP) Transactions. RBI/2011-12/194. September 22, 2011. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/CPS22092011.PDF.

RBI (Reserve Bank of India). 2015. Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks. RBI/2014-15/497. March 11, 2015. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/497OGCC0315.pdf.

RBI (Reserve Bank of India). 2016. Merchant Acquisition for Card Transactions. RBI/2015-2016/410. May 26, 2016. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT410EDB19F37B07A46D9A6192AA99D7B9732.PDF.

RBI (Reserve Bank of India). 2017a. Guidelines on Merchant Acquisition for Card Transactions. RBI/2016-17/296. April 28, 2017. https://www.gujfed.com/uploads/career/0951797001526714599.PDF.

RBI (Reserve Bank of India). 2017b. Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs. RBI/2017-18/87. November 9, 2017. https://rbidocs.rbi.org.in/rdocs/Notification/PDFs/NT87_091117658624E4F2D041A699F73068D55BF6C5.PDF.

RBI (Reserve Bank of India). 2017c. Rationalisation of Merchant Discount Rate (MDR) for Debit Card Transactions. RBI/2017-18/105. December 6, 2017. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11183&Mode=0.

RBI (Reserve Bank of India). 2019a. *Benchmarking India's Payment Systems*. Department of Payment and Settlement Systems, June 4, 2019. https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=923#ANQ.

RBI (Reserve Bank of India). 2019b. *Discussion Paper on Guidelines for Payment Gateways and Payment Aggregators*. Department of Payment and Settlement Systems, September 17, 2019. https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=943.

RBI (Reserve Bank of India). 2020a. Guidelines on Merchant Acquiring Business—Regional Rural Banks. RBI/2019-20/156. February 6, 2020. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT15652ECFBEA7EA34CD4BA0B069A59DEBCFC.PDF.

RBI (Reserve Bank of India). 2020b. Guidelines on Regulation of Payment Aggregators and Payment Gateways. RBI/DPSS/2019-20/174, March 17, 2020. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT17460E0944781414C47951B6D79AE4B211C.PDF.

RBI (Reserve Bank of India). 2021a. Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators. RBI/2021-22/76, August 3, 2021. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOT765729DDE076804962B2A6A35CA343D2F2.PDF.

RBI (Reserve Bank of India). 2021b. "Statement on Developmental and Regulatory Policies." February 5, 2021. https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR105160464FA5D1484207801CF6B4402501C1.PDF.

Republic of Ghana. 2019. Payment Systems and Services Act, 2019. Act 987. https://www.bog.gov.gh/wp-content/uploads/2019/08/Payment-Systems-and-Services-Act-2019-Act-987-.pdf.

Republic of Kenya. 2011. The National Payment System Act, 2011. No. 39 of 2011. https://www.centralbank.go.ke/wp-content/uploads/2016/08/NATIONAL-PAYMENT-SYSTEM-ACT-No-39-of-2011-21.pdf.

Republic of Singapore. 2019. Payment Services Act 2019. https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220.

Safaricom. 2014. Lipa Na M-Pesa Terms and Conditions (2014). https://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/lipa_na_m-pesa_terms_and_conditions.pdf.

Safaricom. 2019. Lipa Na M-Pesa Requirements (2019). https://www.safaricom.co.ke/images/LIPA_NA_M-PESA_KYC_Requirements_2019.pdf.

Safaricom. 2020. *Do More with the M-Pesa Business Till*. https://www.safaricom.co.ke/images/Downloads/Resources_Downloads/M-PESA_BUSINESS_TILL_Booklet.pdf.

SARB (South African Reserve Bank). 2007. Directive for Conduct within the National Payment System in Respect of Payments to Third Persons. Directive No. 1 of 2007. https://www.gov.za/sites/default/files/gcis_document/201409/3026111100.pdf.

SARB (South African Reserve Bank). 2014. "Card Results of the Interchange Determination Project—Phase 2." March 20, 2014. https://www.gov.za/card-results-interchange-determination-project-phase-2.

SARB (South African Reserve Bank). 2016. *Oversight of the South African National Payment System*. https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Oversight.pdf.

SBP (State Bank of Pakistan) 2014. Rules for Payment System Operators and Payment Service Providers. PSD Circular No. 03 of 2014. https://www.sbp.org.pk/psd/2014/C3.htm.

Uzialko, Adam C. 2019. Payment Gateway vs. Payment Processor. Business.com, October 29, 2019. https://www.business.com/articles/payment-gateway-vs-payment-processor/.

Visa. 2011. *Credit Card Schemes in Australia: A Response to the Reserve Bank of Australia and Australian Competition and Consumer Commission Joint Study*. January 2001. https://

www.rba.gov.au/payments-and-infrastructure/credit-cards/iii-submissions-vol2/t1-visa-0101.pdf.

Visa. 2020. Visa Core Rules and Visa Product and Service Rules. Public Version 1.2 (1 June). https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf.

Wadsworth, Jim. 2020. "Why Collaboration and Partnerships Will Beat the Fraudsters in Open Banking." Fintech Futures, June 9, 2020.

Wang, Zhu, Scarlett Schwartz, and Neil Mitchell. 2014. "The Impact of the Durbin Amendment on Merchants: A Survey Study." *Economic Quarterly* 100, No. 3: 183-208.

WB (World Bank). 2005. *AML/CFT Regulation: Implications for Financial Service Providers That Serve Low-Income People*. Focus Note No. 29, July 2005. World Bank, 2005. https://openknowledge.worldbank.org/handle/10986/12495 License: CC BY 3.0 IGO.

WBG (World Bank Group). 2012. *Developing a Comprehensive National Retail Payments Strategy*. Financial Infrastructure Series: Payment Systems Policy and Research, October 2012. http://documents1.worldbank.org/curated/en/839121469729131991/pdf/84076-REPLACEMENT-FILE-PUBLIC-Developing-comprehensive-national-retail-payments-strategy.pdf.

WBG (World Bank Group). 2016. *Cash vs. Electronic Payments in Small Retailing: Estimating the Global Size*.

WBG (World Bank Group). 2019. *Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits*. WBG, 2019.

WBG (World Bank Group). 2020a. *Payment Systems Worldwide: A Snapshot—Summary Outcomes of the Fifth Global Payment Systems Survey*. June 2020. http://documents1.worldbank.org/curated/en/115211594375402373/pdf/A-Snapshot.pdf.

WBG (World Bank Group). 2020b. *Embedding Digital Finance in e-Commerce Platforms during the COVID-19 Pandemic*. Discussion Note. https://doi.org/10.1596/35001.

WBG (World Bank Group) and WEF (World Economic Forum). 2016. *Innovation in Electronic Payment Adoption: The Case of Small Retailers*. WBG, June 2016.


THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP


EUROPEAN CENTRAL BANK