FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

Innovations in Electronic Payment Acceptance

ELECTRONIC PAYMENT ACCEPTANCE PACKAGE

WORLD BANK GROUP

ACKNOWLEDGEMENTS
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 (FIGI) Electronic Payment Acceptance (EPA) Workgroup, funded by the Bill and Melinda Gates Foundation.

This report was prepared by a team from the World Bank Group led by Ahmed Faragallah (EPA Innovations Workstream Chair, Senior Financial Sector Specialist) and including Hemant Baijal (Financial Sector Consultant), Ihab Zaghloul (Financial Sector Consultant), and Louis De Koker (Financial Sector Consultant).

Additional contributions were provided by Nilima Chhabilal Ramteke (Senior Financial Sector Specialist) and Matthew Saal (Principal Industry Specialist, International Finance Corporation), who kindly reviewed this report, as well as by Charles Hagner, who edited the report. Naylor Design Inc. designed and provided graphics for 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 workgroup.

Comprehensive EPA Innovations Workstream consultations were undertaken while preparing and finalizing the report. The workstream comprised Amina Tirana (Visa), Jesse McWaters, Rajiv Mohapatra, and Heba Shams (Mastercard), Ruan Swanepoel (GSMA), Sergey Dukelskiy, Youssouf Sy (Universal Postal Union), Sohail Javaad, Ali Saqib (State Bank of Pakistan), Ma Haoyu (People's Bank of China), Ahmed Monir (Central Bank of Egypt), Elmuez Saber (Central Bank of United Arab Emirates), Martha Hailemariam (National Bank of Ethiopia), Jahongir Aminjanov (National Bank of Tajikistan), Xi Sun (Ant Group), Mandar Kagade (Cashless Catalyst), Gabriela Jaramillo Gabino (CNBV Mexico), Amitabh Saxena (Digital Disruptions), and Vijay Chugh, Oya Pinar Ardic, and Ana Georgina Marin Espinosa (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.

RIGHTS AND PERMISSIONS

Table of Contents

Boxes

Figures

Abbreviations

AML	anti-money-laundering
AML/CFT	anti-money-laundering and combating the financing of terrorism
API	application programming interface
BHIM	Bharat Interface for Money
CDD	customer due diligence
CNP	card not present
DSA	direct sales agent
e-commerce	electronic commerce
eKYC	electronic know your customer
EPA	electronic payment acceptance
e-wallet	electronic wallet
FATF	Financial Action Task Force
FPS	fast payment system
KYC	know your customer
m-commerce	mobile commerce
MDD	merchant due diligence
mPOS	mobile point of sale
MSM	micro and small merchant
NFC	near-field communication
P2M	person to merchant
P2P	person to person
PAN	payment account number
POS	point of sale
PSP	payment service provider
QR	quick response
UPI	Unified Payment Interface
VCN	virtual card number

I. Introduction

1.1 BACKGROUND AND INTRODUCTION TO THE TECHNICAL REPORT

The objectives of this report are to examine the current industry practices in electronic payment acceptance (EPA), review the functioning and value proposition of the emerging payment-acceptance business models and processes, and evaluate leading technological innovations that are influencing the growth of EPA ecosystems in countries that are seeking to promote digital financial inclusion. The report examines the underlying factors that influence innovations and the deployment of payment-acceptance solutions in the context of both traditional and emerging business models with a primary focus on micro and small merchants (MSMs).[1]

The intended audiences of this report are the various stakeholders that have an interest in expanding EPA for MSMs in emerging markets. These include but are not limited to financial regulators, financial institutions, payment service providers (PSPs), mobile-money operators, third-party processors, suppliers and distributors of fast-moving consumer goods, merchants, and technology companies operating in the retail payment market.

The report covers innovations in EPA for retail payment ecosystems. It evaluates innovations within the cards ecosystem, and within the emerging e-money and e-wallet ecosystems, to address the needs of MSMs. In doing this, the report does not compare solutions, business models, and ecosystems or promote one over another but informs the audience of the key features associated with traditional and emerging acceptance solutions tied to each model and emphasizes innovations that have improved the value proposition for MSMs.[2] The report also highlights key enablers for accelerating acceptance among MSMs and captures essential aspects of thought leadership regarding successful acceptance models that have the potential to influence the future acceptance landscape.

The report focuses on electronic-payment instruments used for card-present transactions at brick-and-mortar merchants or during online transactions for the purchase of goods and services using mainly payment cards, mobile money, and electronic wallets (e-wallets). Cards are typically used for card-present (physical point of sale at a merchant site) or card-not-present (CNP) transactions (such as online, teleorder, and other remote transactions) and refer to either a line of credit (credit card) or a current or savings account (debit card). The card is a form factor enabling the use of one's account number to facilitate the exchange of value. It enables customers to

make purchases using the value associated with the card, and it can be linked, in some cases, to additional accounts. In recent years, innovation has led to the introduction of new payment instruments or form factors to facilitate the electronic exchange of value, including electronic money (e-money), an electronic alternative to cash. E-money is a form of monetary value stored on electronic media, such as prepaid cards, mobile phones, and e-wallets, or on a server. *Mobile money*, in this report, refers to an e-money virtual account that can be accessed through a mobile phone and used to make transactions. The report will focus on person-to-merchant (P2M) transactions sent using USSD, SMS, payment applications, or a quick-response (QR) code. E-wallets are merely a container of other payment instruments, such as payment cards or bank or e-money accounts, and can be used online or at a merchant point of sale (POS). In the case of the wallet, the cash value is stored on an electronic device, such as a card, phone, or another device. While *e-money* refers to the value, *e-wallet* describes the receptacle used to hold this electronic value. Other electronic-payment instruments, such as checks, direct debit, and credit transfers through an automated clearinghouse to merchants, were not deeply covered due to their limited usage at merchants or markets.

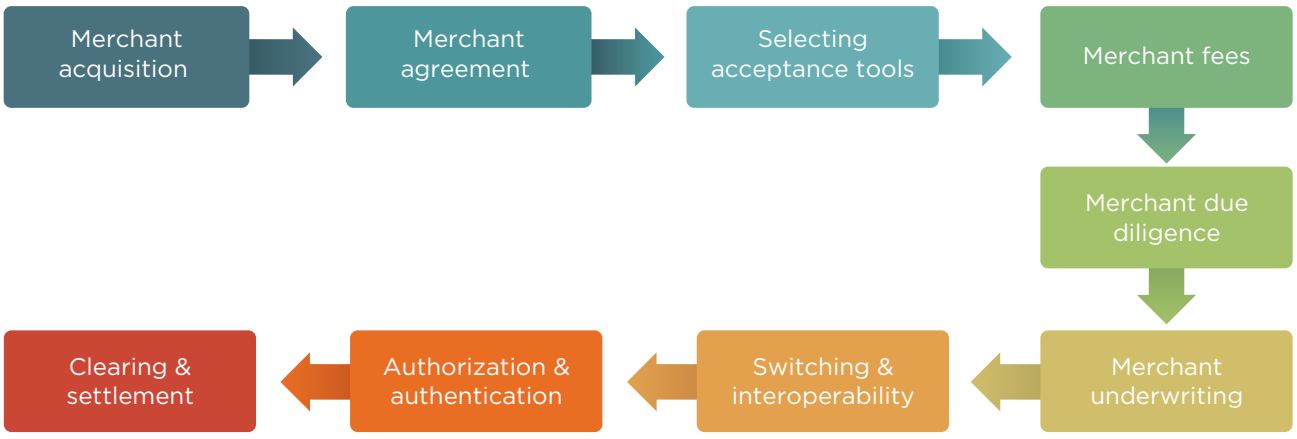
Additionally, the report examines various activities associated with EPA, such as merchant onboarding, authentication, authorization, and clearing and settlement and, wherever possible, illustrates new and innovative methods to implement more inclusive and efficient EPA solutions among MSMs. Based on analysis of good practices and technological and business-model innovations, the report provides recommendations to financial-market authorities and stakeholders for deepening EPA.

1.2 THE DEVELOPMENT OF EPA

The electronic-payment landscape experienced its biggest transformational shift over the past decade, driven by the emergence of new, innovative, and consumer-centric solutions that are not only remarkably cost effective but also quickly adaptable by both consumers and merchants. These solutions are being promoted by policy makers in certain markets who see expanding access to EPA as vital to enabling electronic-payment transformation, which in turn supports economic growth and provides macroeconomic dividends while driving financial inclusion.

The evolution of electronic payments goes back several decades to when the first payment cards were introduced. At that time, they were the only mass-market retail payment instruments available to users for purchasing goods and services. The electronic-payment landscape was dominated by issuer-centric business models that prioritized the issuance of cards over their acceptance by merchants and businesses. As the usage of cards spread, the growth of EPA did not keep pace with the number of cards in the market and was often costly, especially for merchants in emerging markets and the MSM segment. This was primarily because, in an evolving electronic-payment landscape, it is the consumer who needs to be incentivized first to use electronic payment when purchasing goods and services. Solving for acceptance challenges was often a lower priority and was usually dealt with after the consumer's needs were understood and met. This practice resulted in many electronic-payment programs not reaching the desired level of scale and success, despite the large investments. More important, it resulted in reactive acceptance-deployment efforts within various

FIGURE 1: Snapshot of various stages of EPA evaluated in the report[3]



Source: World Bank Group.

merchant segments, leading to a fragmented market-acceptance infrastructure in many markets.

Of late, the focus has been steadily shifting to address this imbalance, and an equal priority is being given to acceptance development. Providers of electronic-payment services realize that an underdeveloped acceptance infrastructure, especially among MSMs, holds back usage and undermines efforts to promote financial inclusion. The other notable trend has been the emergence of electronic commerce (e-commerce) and other forms of electronic payments, such as mobile money and e-wallets. New forms of electronic payments are also contributing to new ways of accepting electronic payments, resulting in increased levels of innovation and specialization in the financial services industry, which in turn is leading to the expansion of low-cost acceptance business models for previously untapped segments, especially MSMs.

Unlike in preceding decades, when only digitally developed markets demonstrated real growth and expansion in EPA and provided best-practice examples for the emerging markets, the opposite is now true. Emerging markets are at the forefront of innovation and deployment of scalable electronic-acceptance models, and all of this is happening in a record time frame. In another notable trend, due to the dominance of cash-based informal commerce in emerging markets and the role played by the MSM segment in it, most new solutions and business models are focused on addressing the needs of this segment and on smaller transaction sizes.

1.3 THE IMPORTANCE OF EPA FOR MSMS

Digitizing MSMs through EPA is a vast step in the efforts to promote financial inclusion. It is estimated that over 180 million MSMs are in developing countries. EPA would not only extend to this huge merchant sector but also cover the 4.5 billion customers who regularly transact with those merchants on a daily basis.[4] The transaction between the MSM and a customer is the last ring in a long chain of trades extending from farmers to wholesale merchants and local distributers. This fact explains the large number of individuals and businesses related to such small retail businesses and the impact that digitizing such chains would have on the economy.

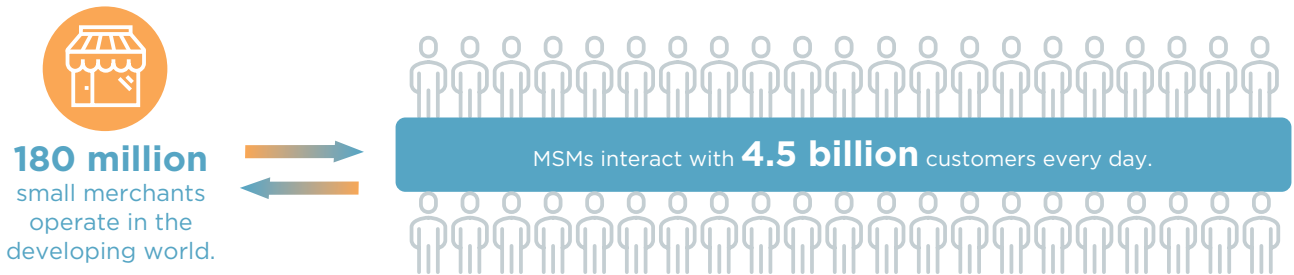
Payments to merchants have always been considered one of the most adopted use cases for the transfer of money. It is estimated that customer payments to MSMs in developing countries amount to $6.5 trillion annually.[5] This huge value could present MSMs with great opportunities to expand their businesses and hire more staff if they had access to finance through loans, credit, and facilities.

The rise of digital technologies offers a once-in-a-generation opportunity to unlock new pathways for rapid economic growth, economic mobility, innovation, job creation, and access to quality services that would have been unimaginable even a decade ago. The accelerating pace of technology diffusion, the convergence of multiple technologies, and the emergence of new business models are disrupting traditional development models. Digitization expands access to basic needs and services. In 2016, the global digital economy was worth $11.5 trillion, or 15.5 percent of global GDP. It is expected to reach 25 percent in less than a decade, far outpacing the growth of the "traditional" economy. Digital financial services, including payment acceptance, are critical enablers of the growth and maturation of the digital economy.

1.4 EMERGING TRENDS IN EPA

As new technologies, business models, processes, and players have emerged over the last decade, the accep-

FIGURE 2: Small merchants are also a big part of the solution for advancing financial inclusion



Small merchants run neighborhood stores that their customer—who are often unbanked—know and trust.

Source: Global Development Incubator and Dalberg, Small Merchants, Big Opportunity (Visa, 2016).

tance landscape has improved significantly, as more MSMs are now able to accept electronic payment. This section reviews some of the emerging trends that are contributing to these changes.

Emerging EPA solutions for MSMs are becoming more mobile-centric, driven by high usage of feature and smart phones. The expansion of mobile phone usage across the globe, including coverage and ownership of smartphones, will continue to facilitate a deeper penetration of mobile money and e-wallet services among consumers and merchants. MSMs are expanding their brick-and-mortar businesses and often integrating e-commerce into their retail point-of-service experience. This has been due to the availability of low-cost acceptance setup and the ability to integrate with easy-to-use e-commerce and mobile commerce (m-commerce) technologies.

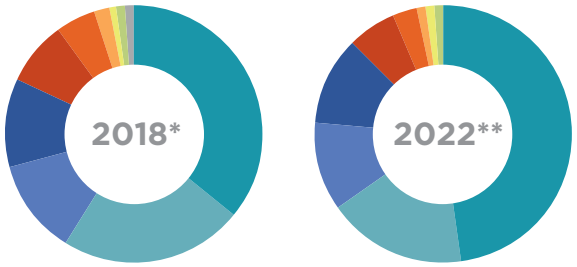
Mobile phones are increasingly becoming the preferred payment instrument for facilitating push payments and enabling low-cost payment acceptance in ways that were not available in the past. For some consumers, the preference to use mobile phones, especially smartphones for P2M transactions, has been made easier due to consumers' ability to link existing payment cards and bank accounts to a mobile or an e-wallet.

For merchants, the process has become equally convenient. They can use a smartphone to register for the service, identify and verify their identity, accept payments, make purchases from suppliers, manage inventory, perform accounting, and much more. The improvements in acceptance by merchants have also played a role, due to wider adoption of mobile point-of-sale (mPOS), USSD, and QR code–enabled technologies, replacing traditional POS devices. The integration of mobile apps into the core business of merchants is becoming a game changer for doing business. Such integration presents huge opportunities for seamlessly integrating payment acceptance into merchants' day-to-day business.

Intermediaries are playing an expanded role in MSM acquiring. More acquirer banks and acquiring service providers are now using intermediaries, such as merchant aggregators or payment facilitators,[6] enhancing their ability to acquire more, new, and different categories of merchants. Intermediaries can provide tailored solutions, outreach, know-how, and good marketing to MSMs. By integrating with banks or microfinance institutions, facilitators and aggregators can provide a more attractive portfolio of products to MSMs.

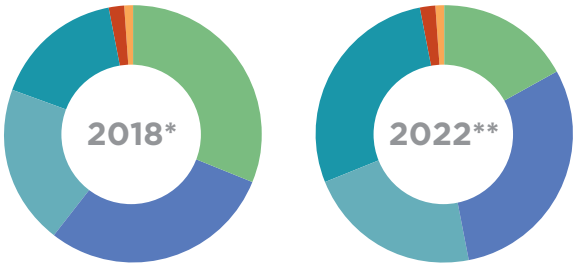
FIGURE 3: Global e-Commerce and Global POS Payments

Global eCom payment methods



	2018*	2022**
eWallet	36%	47%
Credit card	23%	17%
Debit card	12%	11%
Bank transfer	11%	11%
Charge & deferred debit card	8%	6%
Cash on delivery	5%	3%
Pre-paid card	2%	1%
PostPay	1%	1%
eInvoices	1%	1%
PrePay	1%	0%
Other	0%	0%

Global POS payment methods



	2018*	2022**
Cash	31%	17%
Debit card	29%	30%
Credit card	20%	22%
eWallet	16%	28%
Charge card	2%	2%
Pre-paid card	1%	1%

* Estimated
**Forecasted
Numbers adjusted for rouding may impact totals.

Source: Worldpay Global Payments Report.

Acquirers and service providers are providing more "bundled" solutions to attract MSMs. Merchants may not always see the financial benefit of EPA when it is offered as a stand-alone service. However, it is economical for them when a number of financial products are bundled together. For example, supply-chain finance, invoice finance, or a micro credit loan that improves cash flow for MSMs can all be part of a portfolio of financial products that can supplement the EPA. PayTM and Ant Group demonstrate good practices in terms of providing bundled solutions to MSMs. The success is demonstrated in the number of merchants signed up on their platforms.

To grow acceptance in MSM segments, the market is recognizing the importance of push-payment models. The shift toward wider adoptions of e-wallets or QR code is creating new acceptance ecosystems. The shift to acceptance models in which the payer pushes the transaction—rather than the payee (merchant) pulling the funds, as in typical card schemes upon usage at the POS terminals—is reducing the liability of fraud and improving the value proposition for MSMs. The impact of this shift is to eliminate the need for expensive POS terminals with PIN-acceptance features and minimize the need to assess the credit risk of the merchant and, hence, to further the ability of acquirers to accept merchants with little or no credit history. In addition, merchants will be readier to engage in EPA, as funds are credited to their accounts instantly or on the same day, and due to the low risk of chargebacks. Low fraud risks may also encourage acquirers to reduce the merchant service fee, thereby making the cost of acceptance a lot lower compared to the traditional models. A cheaper engagement process will encourage more merchants to join.

Emerging payment solutions are supporting instant, real-time, and fast payments. The fast payment settlement feature is a key driver in expanding push-payment solutions. Fast payments are incentivizing MSMs to accept electronic payment due to instant or nearly instant settlement times. While the typical acceptance cycle using cards was unsuitable for many MSMs because it breaks the cash-flow cycle for merchants, the shift to real-time settlement with access to funds to pay for suppliers gives merchants a true alternative to cash. The payment solution providers should work on providing added value to merchants by expanding the use cases and merchants' level of integration to their list of suppliers, partners, and service providers. For a taxi driver, this list may include mechanics, a garage, gas stations, insurance, and spare parts. For a small shop, the list may include goods suppliers and access to wholesale markets or domestic markets. Domestic providers of solutions should be able to make the proper list of connections to the merchants and link the merchants to their prospective customers through advertising and merchandising support. It is crucial for every link in this chain to be connected to a back-end fast payment system where funds can flow easily, on time, and with reasonable fees.

As an outcome of new business models as well as industry-led merchant-segmentation efforts, the cost of accepting electronic payments has generally decreased for MSMs. Targeted industry-led initiatives to promote merchant acceptance in MSM segments using a combination of special pricing and subsidized POS or mPOS terminals have produced a higher uptake among MSMs. Additionally, the emergence of low-cost smartphones and the wide adoption of QR code solutions have helped enable the fast, cost-effective, and scalable growth of merchant acceptance in new geographies and new merchant segments. In either person-to-person (P2P) or P2M models, transfers via mobile money are cheap. The service providers tend to create revenue streams from the floating cash, add-on services, transfers to other providers, and further credit or saving services with merchants. As a result of these trends, more merchants are willing to accept electronic payment and encourage their customers to use it for payment.

Know-your-customer (KYC) screening, underwriting, and compliance processes are being automated. To accelerate merchant acquisition for the MSM segment, service providers are increasingly utilizing automated underwriting software to enhance the speed, cost, and time to market for onboarding merchants. The challenge for existing and new providers is to strike the right balance between gaining market share and not compromising the quality of underwriting.

Alternative data tools for evaluating MSM creditworthiness have become critical in extending financial services to MSMs at a low cost. Using alternate data-based methods for evaluating creditworthiness, based on merchant categories and such nontraditional data elements as mobile and utility bill payments, and applying simplified due diligence to register small merchants can all lead to a faster, cheaper, and risk-controlled engagement processes. This will improve the ability of MSMs with little or no history of access to financial services to receive such services on a fair basis.

Domestic fintech service providers are gaining traction by providing localized solutions. The expansion of acceptance into new and nontraditional merchant segments will require local community knowledge to develop local-

ized solutions that meet the merchant needs and provide incentives to move away from the informal economy. The targeted capacity building of merchants can help drive literacy and usage. Product localization can also build in relevant aspects related to the legal and regulatory framework, domestic experience, and religious and social norms. The success of service providers will depend on their ability to solve domestic or local challenges. For example, in some Islamic countries, typical credit is not widely accepted. Hence, many providers changed the terms and conditions to apply penalties as an alternative to applying interest on due payments. In countries where credit cards are not widely used or issued, using debit cards or mobile money provided a good alternative for acceptance. Domestic service providers may provide the opportunity to local MSMs to expand the customer base beyond physical and domestic boundaries.

The use of digital ID for merchant verification is growing. Applying simplified due diligence and remote identification and verification measures for individuals and MSMs accelerates financial inclusion and expands EPA. For instance, the use of biometrics to build a digital profile for unbanked merchants in India has enabled faster deployment and adoption of the new digital-payment solutions by consumers and merchants. The success of Aadhaar digital ID solution, and its integration with financial services, allowed digital ID–based solutions for merchants' KYC verification to be leveraged easily. In Pakistan, the State Bank of Pakistan allowed small merchants to open bank accounts using the business owner identification and verification.

A stronger case can be made among regulators for promoting interoperability in payments. There are many dimensions of interoperability, including the ability to exchange financial transactions among different service providers, through different channels, and via different payment instruments. There is a huge benefit from promoting domestic as well as cross-border interoperability. While international and domestic card schemes have developed standards for interoperable acceptance, efforts are underway to expand interoperability among other acceptance models and across channels. Some countries are developing interoperable mobile-money platforms to enhance the merchant acceptance use case. Providers of QR code are developing standards to promote standardization and interoperability[7]—with successful examples from Hong Kong, India, Malaysia, and Singapore showing a paradigm shift toward developing acceptance. The limitations of closed-loop payment solutions are driving dialogues on the need to foster better stakeholder collaborations on interoperability, realize the next stage of growth, enable wider cross-border payments, and reduce the costs of replicated infrastructures. This will facilitate faster digitization and enable financial inclusion.

The markets are working with various industry partners and adopting more inclusive messaging and data standards to accommodate a diverse range of business models. Markets tend to develop and follow messaging and data standards to overcome market fragmentation and promote interoperability. The development of the QR code–based EMVCo standard and the extended use of ISO 20022 for fast payment systems show the need to integrate and interoperate among market players. Further standards for using application programming interfaces (APIs) are being adopted for retail payments. The work on developing and expanding standards allows new providers to access the infrastructure and interoperate with other providers based on preset rules for exchanging data and financial information while preserving a high level of security.

1.5 MAJOR OBSTACLES IN EXPANDING MERCHANT ACCEPTANCE

Despite the promising growth seen in the adoption of electronic payment in the last decade and its potential to have a deep impact on inclusive growth, the progress has not been universal, and a lot needs to be done in markets that are still entrenched in cash-based economies. Key obstacles impede progress, especially in emerging markets, and policy makers should understand the implications and design policies that help address them.

A strategy for addressing obstacles to the expansion of EPA has to be designed and implemented at an individual market level, as the same solutions may not be relevant across markets due to differences in retail payment infrastructures, regulatory environments, investment levels, and the capacity of local players; cultural factors; user base and predominant use cases that influence the merchant value proposition; and the merchant's awareness of the benefits and willingness to adopt. Further challenges may also influence the strategy if a large number of targeted MSMs are in remote and rural areas.

The traditional POS-based acceptance solutions involve both fixed costs and costs per transaction. The fixed costs can be justified for mid-size to large merchants that have high sales volumes and the operational capacity to implement such solutions and also be compliant with industry standards for data security.[8] The transaction costs may be acceptable if acceptance leads to more customer traffic, higher sales amounts, or counterbalancing savings in cash handling, shrinkage (for example, staff pilfering), and other costs. However, smaller MSMs are unlikely to see a positive balance with

traditional solutions, due to unfavorable transaction economics and the high costs of setting up and operating such devices. As more cost-effective solutions with faster processing times become available, the focus is now shifting from addressing the cost challenge to finding the right local market approaches to grow acceptance among MSMs. These include merchant acquisition, underwriting, and onboarding, as well as overcoming financial literacy and capacity-building challenges.

To enable MSM communities to be active participants in the formal financial sector, their pain points, interests, and material issues with the EPA value chain must be understood well and addressed adequately. Many MSMs in emerging markets operate in the informal financial sector, have never had a previous relationship with a bank, have little awareness of the financial products and services offered by banks, and may not have access to the internet. Even banks do not see them as potential customers, as the MSMs typically do not qualify during the KYC due-diligence process and can afford neither to pay high transaction fees nor to receive their money late if accepted electronically.

The key obstacles to expanding acceptance of electronic payment for MSMs can be summarized in four categories: economics and value proposition for MSMs; low priority for traditional service providers; technology, risk, and regulatory constraints; and other factors that create friction in the adoption of electronic payment.[9]

1.5.1 Weak Value Proposition for MSMs

Most MSMs do not see a compelling value proposition for accepting electronic payment over cash. This is due to the following factors:

- High up-front and ongoing costs of acceptance. MSMs do not have to make any up-front investments to accept cash from their customers. It is also unclear to these merchants how they will attract new customers or sell more goods to existing customers by accepting electronic payment for the low-transaction-value items that they deal with predominantly. For these reasons, they prefer cash, as it appears to have no cost and may even save them money through a lower tax bill, while a move to electronic payments could provide an audit trail and expose merchants to tax liability.
- For traditional card-based models, the time it takes for funds to transfer to a merchant's account is unattractive for MSMs. It can take two to three days on average for final settlement, and MSMs that are generally strapped for working capital cannot afford this delay. These merchants typically use funds from today's sales to buy stock for tomorrow's business. This can present a challenge also for newer forms of electronic payments that clear instantly. Moving funds between cash on hand and e-money balances may require a trip to an agent or bank branch. Thus, if both forms of payment are accepted, the merchant may have to maintain extra liquidity to pay suppliers that accept only one or the other form of payment.
- Regulatory requirements in terms of KYC and other documents needed for authorizing a new merchant to accept electronic payment can be particularly cumbersome and expensive for MSMs, since many may lack proper proof of identity or may not be registered businesses.
- Cash-management practices used by merchants have them using physical cash for budgeting (for example, keeping separate envelopes for this month's rent, wages, and supplies) and saving. If the e-wallet does not provide similar functionality, it can disrupt habitual, though basic, cash-management practices, decreasing, rather than increasing, a proprietor's perceived efficiency.

1.5.2 Low Priority for Traditional Service Providers

Some service providers, upon starting work in a new market, focus on addressing consumer needs on the issuance side and focus on merchants and the acquiring side later. From a marketing perspective, service providers need to establish a mass consumer base to be able to convince merchants of the value of the service. Meanwhile, most service providers concentrate on large merchants. In terms of priority, MSMs have typically fallen behind other segments in most markets for driving growth of electronic payment.

Making up-front investments to grow acceptance in the remote rural locations where a large number of MSMs operate is a low priority for service providers. Instead, they focus on large cities, competing mainly on price to win merchants, rather than opening up new merchant-acceptance channels to serve the financially excluded.

Banking practices in many emerging markets also tend to focus primarily on the cash-management business of large merchants, and acceptance is generally seen as a value-add product.

1.5.3. Technology, Risk, and Regulatory Constraints

Poor information and communications infrastructure and little or no financial incentives for service providers to invest in remote rural areas, where the transaction volumes are low and the affinity for cash is high, often create obstacles for growing the acceptance network outside high-density urban centers.

Within the traditional practices, a lack of effective mechanisms to conduct proper due-diligence and KYC protocols for remote and rural merchants can increase costs that are unattractive for the acquirer.

1.5.4 Other Factors

Low financial literacy among remote and rural merchants results in a lack of trust in unfamiliar electronic-payment solutions and a continued preference for cash-based transactions. Among consumers and merchants in many markets, cash has greater familiarity and trust than electronic payment.

2. Merchant Acquisition and Agreement

2.1 MERCHANT ACQUISITION

Merchant acquisition is an integral part of processing electronic-payment transactions. In the merchant-acquisition process, acquirers enable merchants to accept electronic payment by acting as a link between merchants, issuers, and payment networks, providing authorization, clearance and settlement, dispute-management, and information services to merchants.[10] An acquirer signs a merchant-acceptance agreement with the merchant that includes details of the required minimum service standards to be provided by the acquirer and terms for transaction processing, invoicing, chargeback and settlements, fees and costs, technical support, value-add services, and other policies applicable within the market or merchant segment. The merchant acquirer can be a bank or a non-bank entity. The merchant-acceptance agreement can be signed with the acquirer or with a merchant aggregator or facilitator

Depending upon the relationship with the acquirer/merchant aggregator/facilitator and the availability of solutions in a given market, the merchant may accept one or multiple forms of payment cards; mobile and e-wallets from one or more brands using a QR code or the near-field communication (NFC) protocol; and either online or using one or more physical acceptance devices. Some card schemes apply the "honor all cards" rule, which requires merchants to accept all types of products as a condition of accepting their brand.

The drivers behind the acquisition of MSMs are different from those behind the acquisition of large merchants due to the economies of scale and the risks associated with this segment. During the acquisition process, considerations have to be made for merchant location, available technology and information and communications infrastructure, and merchant and consumer literacy levels, including awareness of fraud risks, cash-dominance levels, local regulations, cultural norms, and the electronic-payment solutions that are likely to be used at the merchant.

For these reasons, a successful acquisition strategy for MSMs requires careful planning, preparation, and targeting of the merchant segment. To grow acceptance for MSMs, the service providers must understand the needs of the segments and address their pain points effectively by offering solutions that conform to their needs.

2.1.1 Merchant Selection

The merchant-selection process is usually driven through an acquirer strategy that has predefined goals and objectives for increasing penetration and improving scalabil-

ity within a merchant segment. The goals usually define merchant targets within specific geographies, merchant industry verticals, timelines, and predefined revenue and expense drivers.

2.1.2 The Role of the Direct Sales Team and External Direct Sales Agency

Depending on the merchant segment, scale, and geographic distribution, the merchant-selection process can be carried out either by the direct sales team of the acquiring entity or by an outsourced third party, also known as a direct sales agent (DSA), contracted to carry out the merchant-selection process. The approach is typical within the cards business.

As part of the prescreening process, DSAs identify the prospective merchants and persuade them to accept electronic payment by explaining the merchant value proposition, fees and costs, fraud-prevention best practices, chargeback process, and other relevant payment-acceptance terms and conditions. If the merchant agrees to become an acceptance point, the DSA collects the information required for the acquiring entity to conduct the KYC process necessary to make an underwriting decision. The DSA is also responsible for the signing of the merchant agreement, account opening, and ongoing communications with the merchant. The acquiring entity's direct sales team may manage one or more DSAs in the region. The direct sales team may also deal directly with key merchants and assist in the terminal deployment, as required.

2.1.3 Important Considerations for the Merchant-Selection Process

Lessons learned in the merchant-selection process for MSMs in developed markets point to the need for a localized merchant-selection strategy to ensure its effectiveness. The selection of qualified DSAs with local knowledge will ensure that the initial merchant-solicitation process is an effective one. Once the merchants are onboarded, the DSAs can help with ongoing communication and financial-literacy efforts to ensure that merchants are educated on the benefits of EPA. Such efforts are critical to widespread adoption and increased usage of electronic payment.

Providing appropriate revenue incentives to the DSAs for merchant selection, in the form of a fee per merchant signed, may also increase the number of merchants acquired.[11] However, the selection process alone does not ensure that these merchant accounts will remain active. To ensure low dormancy rates, it is critical to provide the right mix of incentives and education within the value chain, especially to those who are in the business of maintaining regular contact with the merchant community.

In addition to providing the right incentives within the value chain, the successful acquisition of merchants also depends on the readiness of market infrastructures, an enabling regulatory policy environment that simplifies the customer due diligence (CDD) process, and consumer demand for and the corresponding availability of digital payments. From the merchant perspective, an uptake in digital payment by consumers versus cash may affect a merchant's ability to manage its suppliers that accept only cash, so the value proposition for going digital must hold throughout the merchant supply chain for it to work effectively. For this, it is important to leverage the expertise of large global corporations that extend their supply chains to informal MSMs in developing markets.

2.2 BANK-MERCHANT AGREEMENTS

TYPICAL MODELS

2.2.1 Merchant-Acceptance Agreement (Network Model)

The merchant agreement is a legal contract that regulates the relationship between the merchant and the acquiring bank or the acquiring service provider/merchant aggregator/facilitator to accept electronic payment. This is the typical model for merchant setup in the case of network-branded payment solutions, such as Visa, Mastercard, and China Union Pay.

The merchant agreement indicates the types of payment-related services the acquiring bank or service provider will offer to the merchant and details the responsibility of the merchant in complying with EPA rules set by the payment brands. The merchant agreement clearly stipulates the merchant transaction fees and provides details on the transaction chargeback and settlement processes.

American Express, which follows a three-party model (described in section 4.2), may develop a merchant agreement with the merchant directly, or it may follow the payment network acquirer model by outsourcing the merchant-acquiring services to an acquiring bank or a licensed acquiring entity.

NEW MODELS

To achieve merchant-acquisition goals, merchant acquirers apply different models to accelerate recruitment. Examples below demonstrate some of the innovations happening in this space.

2.2.2 The Merchant Payment Facilitator Model

A payment facilitator is a merchant service provider that simplifies the merchant account enrollment process. In a payment facilitator model, the payment facilitator (or a merchant aggregator) signs up merchants directly under its own merchant ID number to process transactions through a single master account. Contrary to the traditional model, in which an acquirer provides a merchant account to each merchant, this approach uses just one merchant account to represent many merchants. In this respect, the acquirer is able to achieve a faster time to market for merchant acquisition and onboarding.

In a typical setting, a payment facilitator will sign a sponsorship agreement with an acquiring bank and obtain a master merchant ID account. This includes administering an application and underwriting process, working out a pricing agreement, and facilitating payment technology integration for the merchant. The acquirer is then responsible for monitoring the payment facilitator's compliance with operating regulations, including KYC and anti-money-laundering (AML) requirements, and ensures that proper due diligence is being carried out when onboarding submerchants. The payment facilitator undergoes a comprehensive process to register with an acquirer, including the integration process.

Next, the payment facilitator will sign up the submerchants. As an example, an MSM applies for a submerchant account by providing a few data points to determine eligibility. These data points are then evaluated by using an underwriting tool, and the decision to onboard the MSM is made in a short amount of time (in near real time in some markets). Once approved, the merchant is onboarded as a submerchant on the payment facilitator's merchant ID account. The payment facilitator assumes all risks and liabilities for its submerchants. The payment facilitator settles and disburses payments to the merchants on its submerchant platforms.

Once the submerchant volume of transactions reaches a certain threshold, the submerchant may be required to move off the payment facilitator's platform and obtain its own individual direct merchant agreement with the acquiring entity.

The greatest benefits of the payment facilitator model are its ability to offer faster merchant onboarding, deliver wider merchant reach, apply domestic experience, and simplify and streamline the merchants' account-enrollment and onboarding process by leveraging the technology to a wide range of merchants, including mPOS devices, mobile apps, and online payment-processing gateways. The fee structure and technology used by payment facilitators vary by market and depending upon the maturity of the market.

Payment facilitators may also offer services under their own brand (for example, Square) and offer a complete white-label payment-processing solution. This ultimately leads to more control over the processing experience, higher merchant conversion rates, and the opportunity to earn more revenue from card processing. The disadvantages to this approach are that it increases the payment facilitator's level of responsibility for fraud, chargebacks, and data breaches, the resources to build or purchase payment technology, and the ability to meet compliance mandates and regulatory rules to register as a service provider validated at Level 1 or Level 2 of the Payment Card Industry Data Security Standard (PCI-DSS).

The ability to onboard merchants smoothly using quick automated underwriting decisions is becoming a key value proposition for the payment facilitator model. This is critical to keep merchants from abandoning the merchant-acquisition process due to a lengthy and cumbersome application process and the slow underwriting decision-making process usually associated with traditional acquirer models. Square's entire business model is built around fast, convenient merchant onboarding.

The payment facilitator model could be more suitable for medium to small merchants. This model is particularly effective in the recruitment of medium to small merchants, breaking down the barriers of connections between traditional banks and individual small merchants. Merchant facilitators are important partners that accelerate the inclusion of small merchants and financial-inclusion efforts.

2.2.3 The Payment Gateway Model

Today, both e-commerce and smartphone-enabled m-commerce are essential to the success and growth of many large, medium, and small merchants' businesses. E-commerce transactions continue to grow year over year;

Amazon is another large payment facilitator that also acts as a merchant of record. Unlike PayPal, Amazon makes itself the merchant of record no matter the size of the submerchant. That's because consumers are choosing to purchase from the submerchant through Amazon's platform, and it makes the most sense for Amazon to appear on their bank statements.

Fawry is an e-payments platform in the Arab Republic of Egypt providing merchant-facilitator and bill-payment services. In partnership with Egyptian banks, Fawry also provides the technology solution for acceptance of e-wallets. Fawry has over 165,000 locations (agents, ATMs, and retail locations) and multiple channels (online and face to face) that allow customers to use both cash and non-cash means to pay bills, top up their mobile phone credits, donate to charities, pay school tuition and fees, and settle bills for "cash-on-delivery" e-commerce orders. Fawry's network of retailers includes small grocery and convenience stores, pharmacies, stationaries, and post offices, all equipped with POS terminals. It has recently extended its services to provide merchant-acceptance services, including working-capital loans and other merchant services. The lending component is important, as it provides the working-capital loans that small and medium-sized merchants use to grow their businesses, and in return, they become an EPA point.

Blue Label is a financial technology company in Mexico that provides merchant-facilitator and EPA services to MSMs under the trademark Red Qiubo. Its network is the largest of its kind in Mexico. Blue Label provides mPOS terminals to MSMs that can accept payment cards, social protection and food vouchers and cards, utility and bill payments, and airtime recharges. Consumers using airtime recharges and bill- or utility-payment services must download the Red Qiubo app to initiate the payment transactions. The company also has a special app that enables payments from merchants participating in various supply chains (for example, Grupo Bimbo). This allows merchants to settle their outstanding balances directly with Grupo Bimbo for the bakery products sold by them. The process for onboarding small and medium-sized merchants is simple. For unbanked merchants, Blue Label also helps to open a bank account for receiving their payments. Merchants, on the other hand, receive a commission for accepting bill or utility payments and airtime recharges.

the global online sales reached $3.53 trillion by 2019.[12] In addition to any card-present services a payment gateway provider may offer, payment gateways enable merchants to conduct CNP transactions using online or mail or telephone channels for different types of cards and digital payment account wallets. The payment gateway acts as an intermediary between the online store and acquirer entity. The payment gateway can perform additional services, including fraud detection, money-laundering list lookup, delivery address verification, and tax calculation. Digital and e-wallets accounted for 42 percent of e-commerce traffic by 2019.

The growth of e-commerce and m-commerce has led to the popularity of payment gateways by enabling merchants to accept different types of e-wallets, CNP transactions, or mail- or telephone-order payment requests.

Gateways offer both consumers and the merchant secure transaction processing, mitigating the risk of fraudulent incidents. They can also process multicurrency cross-border transactions, provide integration options with large merchants' e-commerce platforms, and allow real-time insights on current and future payment trends through data analytics reporting.

The retail e-commerce market will continue to grow as more and more businesses adopt payment gateways to help restructure and drive revenue growth. The fast growth of e-commerce and m-commerce has led to an urgent need to deploy online merchant-acceptance solutions that are simple, fast, secure, and cost effective.

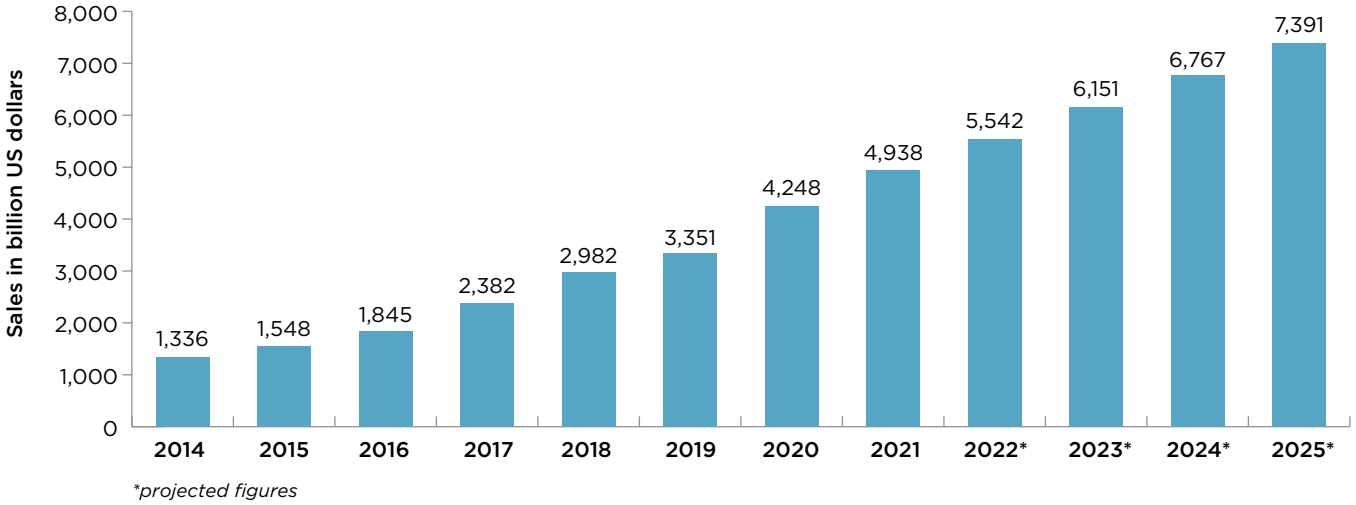
2.2.4 The Mobile-Money Acceptance Model

A mobile-money payment service is the transfer of funds from one mobile-money account to another and is initiated using a mobile phone.[13] Since the launch of mobile-money services over 10 years ago, they have evolved from facilitating mainly P2P transactions to becoming a more prominent payment-acceptance method, displacing traditional POS solutions in certain markets.

A merchant transaction on a mobile-money service, also known as a P2M transaction, works like a P2P transaction. In a P2M transaction, the recipient is a merchant that receives payment from a consumer either as a normal mobile-money P2P transfer or using a credit-push model based on a QR code. In payments through a QR code, the consumer simply scans the merchant's QR code (two-dimensional barcode) and enters the transaction amount to complete the transaction.

Some mobile-money services also employ "pull payments" to make it convenient for customers. In a push

FIGURE 4: Retail e-Commerce Sales Worldwide, 2014–21 (US$, billions)



Source: Statista 2022

M-Pesa: For P2P and P2M transactions, M-Pesa uses the SMS method for payments. Registered customers deposit cash in exchange for electronic money at an agent and use SMS to make purchases and send money to other users. A user must enter a PIN to initiate a transaction, and both parties receive an SMS confirming the amount that has been transferred. The recipient, who does not have to use the same network, receives the electronic money in real time and then either redeems it for cash by visiting another agent or spends it at an M-Pesa merchant. M-Pesa is also available as an option for online payments for e-commerce purchases and utility bills.

Ecocash is the mobile financial service available to Econet customers in Zimbabwe. Initially, Ecocash started as an SMS-based P2P payment service but has transitioned into a QR code–enabled digital wallet platform. For P2M payments, merchants who are registered as Ecocash merchants can accept payments from consumers using the QR code. The QR code payments are push payments initiated by consumers at the merchant location.

payment, the customer enters the full transaction details, while in a pull payment the customer enters only the PIN (the secret code), which is inherently riskier. To mitigate this risk, mobile-money systems in South Africa (including MTN and TYME) and Indonesia (XL) employ a hybrid system that requires customers first to request a one-time password through their mobile device to authenticate the transaction at the merchant terminal. A third option for the transaction processing is the request-to-pay protocol, which is becoming popular with the emergence of fast payment systems: The merchant enters the transaction information and sends it to the customer's terminal. In response, the customer has to initiate a new transaction from the customer's terminal using the information received from the merchant.

Another pull-payment method employed by mobile-money providers is linking the mobile-money account to a physical or virtual card number of a payment network. The "physical" companion card follows the card rails for the transactions at merchant POS terminals. Zuum in Brazil and MiFone in Mexico are examples of such offerings. In other markets, some providers also provide a "virtual" prepaid card that can be used for e-commerce transactions. Orange in Egypt uses this approach.

In a typical mobile-money model using SMS or USSD protocols, merchants accepting payments act as agents. Hence, they can use the same pool of mobile-money funds to cash in or out or sell products. ZAAD mobile money in Somalia has deployed 12,300 registered merchants that are 89 percent active. Mobile money is expanding and is

bKash is a mobile financial service in Bangladesh offered by BRAC Bank. Since its early days, the bKash payment service has been USSD based, and there are 47,000 merchant acceptance points that accept payments from consumers. For a USSD payment, users must enter the payment-specific code, merchant bKash account, and other user-specific information to complete the transactions. Smartphone users also have the ability to download the bKash mobile app to manage the account and initiate transfers and payments. Several retailers in Bangladesh also allow consumers to use their bKash wallet for e-commerce.

The case of **PayPal** is somewhat different from Square. PayPal is a classic example of a payment facilitator, or a master merchant serving a number of small submerchants. Consumers know and trust PayPal, so when they use their payment card at an unfamiliar small merchant, they are not concerned about sharing their card details—they just pay through PayPal. Since PayPal is the merchant facilitator, bank statements show PayPal as the merchant on record, and the transaction is then relayed to a submerchant. In that case, PayPal is both the payment facilitator and the merchant of record.

now available in 90 countries, becoming a relevant key digital-payment solution used by 690 million account holders in 2017.[14]

As the demand for mobile-money acceptance increases, the economics of merchant transaction acceptance continues to be a key area of focus, as it directly and partially influences the speed of merchant-acceptance expansion. Mobile money is growing in different stages in different countries, and despite the rise of smartphones, phones running the USSD protocol and feature phones remain in wide use in emerging markets, supporting the overall growth and usage of mobile money. As the demand for mobile-money acceptance increases, the fees and costs associated with mobile-money acceptance become a key focus area.

To boost mobile-money acceptance, **Kopo Kopo** introduced a scheme in Africa in 2014 by which they provide microcredit to 12,500 merchants that are enabled as mobile-money acceptance points across Kenya, Rwanda, and Tanzania. The more digital transactions these merchants process, the greater the loans they qualify for; the loans can be repaid as part of the merchant's commission. As a result, merchants typically prefer electronic payments and advocate for consumers to use them, thereby driving up usage.

2.3 RECOMMENDATIONS

- Regulators should establish a level playing field for banks and non-bank service providers to provide various types of EPA solutions and services.
- Regulators should encourage innovations in EPA by allowing the participation in the acceptance value chain of various types of intermediaries, such as payment facilitators, merchant aggregators, and non-bank merchant acquirers. Provisions should be made to allow such non-bank entities to become viable acceptance service providers. (See the example below.)
- Regulators should employ the right blend of regulations to encourage innovation, mitigate risks, and promote public-policy objectives that support financial inclusion, competitive market conditions, and consumer protection.
- In emerging markets, regulators and industry stakeholders may consider all acceptance methods by providing a level playing field to all providers, including alternate solutions that leverage mobile-payment technologies.
- Providing tax and other forms of incentives to merchants can help facilitate easy adoption of QR code–based mobile payment acceptance, such as in India for use of QR code for Unified Payment Interface (UPI) payments.

- When developing solutions, service providers need to categorize the merchants based on their business, size, market conditions, and possibly other factors to develop acceptance products, solutions, and pricing models that meet the needs of MSMs and address their pain points.
- Acceptance in some markets may not be a product sold solely to merchants but should be bundled with other products to make it attractive for MSMs, including lending, supply-chain and invoicing finance, and possibly insurance. Authorities could allow the sharing of merchant data/information with licensed entities, with merchant consent, to provide such services and other forms of acceptance

3. Selecting the Merchant-Acceptance Tool

TRADITIONAL MODELS

The typical merchant-acceptance operation requires retail POS terminals that may include an electric cash register or an integrated computer system that records the data associated with a business transaction for the sale of goods or services. The hardware and software components may include retail merchant system terminals, POS devices, card readers, merchandise scanners, card scanners, printers, PIN pad devices, radio-frequency identification or contactless terminals, system software, telecommunication lines, wireless connections, or any other hardware.[15]

The choice of hardware and software used by a merchant depends on what is available in a given market and the ability of local or national information and communications infrastructure to support the technology. Selection also depends on the preferred use of payment types by the merchant's clientele, the nature of the business, merchant size, and, if the merchant has a store, whether it is an online merchant or a multichannel business.

The connectivity options will also vary according to the merchant business model, which can range from an IP/VPN requiring internet connections to wireless solutions requiring cellular network connections or dedicated leased lines for large-volume merchants. Merchants are typically looking for PSPs that can provide terminals that are PCI-DSS compliant and can process different payment types, including credit, debit, gift, and loyalty cards, or accept P2M transfers and QR code–based solutions for mobile payment.

Traditional acceptance terminals provide processing choices for swipe, chip and PIN, and contactless payment readers. The merchant priorities are typically centered on cost, customer convenience, processing speed, security, reliability, built-in printers, wireless capabilities, and service quality. MSMs traditionally process transactions end to end on a POS device, while large merchants may have more sophisticated hardware and software setups linking PCs, checkout registers, PIN pads, and others to transmit accepted transactions to the acquiring service provider.

NEW MODELS

Most of the developments in payment acceptance emerged from the need to reduce the EPA cost or to provide more convenience to the consumer. The mPOS terminal was an alternative to the traditional POS terminal, where the acceptance peripheral (card reader) is plugged into a smart mobile. The mPOS terminal could accept cards for swiping, chip reading, or connecting to a contactless card, based on the card and mPOS technologies.

Mobile acceptance is the simple transfer from a consumer's mobile-money account to a merchant's mobile-money account. (Both are e-money accounts.) In terms of functionality, it is similar to P2P transfers, where the recipient is the merchant.

Acceptance through QR code is performed via a mobile or hand device. QR code is a two-dimensional barcode that contains the merchant's (or buyer's) financial information, including a bank name and account number. The QR code could be static (a QR code printed on paper and placed on the merchant's shelf) or dynamic—that is, a QR code on the merchant's mobile phone that facilitates the transfer of funds to the merchant's account.

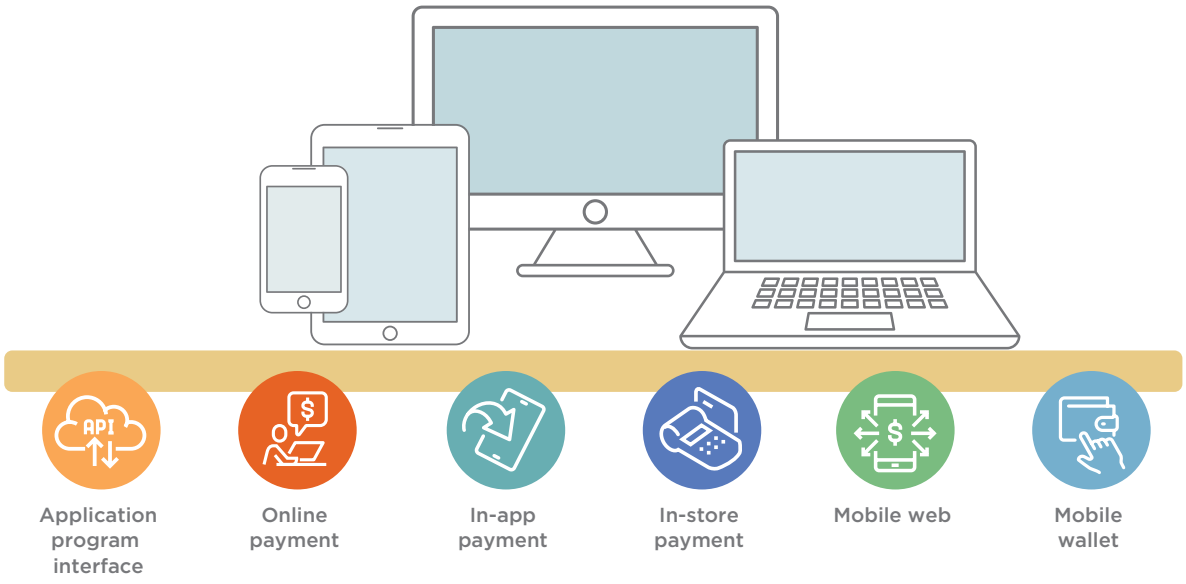
e-Wallets are mobile- or computer-based applications that facilitate payments to a merchant based on the merchant's provided information. The customer initiates a transaction from the customer's device by entering or retrieving the merchant's information, while the e-wallet will use the customer's account information to make the payment. E-wallet transactions could be credit push or credit pull based on the application provider and the rules of the governing payment scheme among the service providers.

Finally, contactless acceptance of cards and e-wallets, through NFC technology, is becoming significantly important to facilitate social-distancing measures. The following sections detail some of the modern acceptance tools.

3.1 MERCHANT mPOS

An mPOS system is a portable POS solution on a smartphone or tablet that functions as a cash register. Presenting a smart cost-effective alternative to the traditional POS device, it can accept different forms of payment. A generic mPOS system consists of a card reader that is paired with a smart device such as a smartphone or tablet either wirelessly or physically and uses the wireless or mobile phone's data connection to process transactions. To process transactions, a merchant must download the relevant mobile app provided by a merchant service provider. Reusing a device that the merchant already owns, with its own connectivity, obviates the need for a new device and phone line for the mPOS system and reduces the cost of acceptance and provides the merchant with new customer-engagement opportunities.[16] From an MSM's perspective, mPOS technologies that utilize smartphones, tablets, and PDAs are growing in popularity, particularly for MSMs needing a low-cost way to accept electronic payment. In comparison to traditional POS terminals, mPOS solutions offer distinct advantages for smaller merchants,[17] including lower total cost of ownership without fixed monthly fees, portability and easy setup and use, simple user interfaces for both the merchant and consumer, easy online reporting to track sales and issue refunds, if needed, and flexibility to fit any type of business. With contactless payments and e-wallets increasing in popularity, mPOS systems are also better equipped to accommodate those customers who simply wish to tap their phone to pay.

FIGURE 5: Merchant-Acceptance Tools and Payment Options



Source: Alte group.

Examples of Successful mPOS Deployments[18]

The **Bun Bun Truck,** a mobile food vendor in Sweden, significantly reduces its operating costs by accepting card payments with a tablet and an iZettle mPOS solution. During peak business hours, Bun Bun employees pair the iZettle chip card reader with a tablet using Bluetooth, and the mPOS is ready for service. To manage cash flow and finances, the owners of Bun Bun log on to the iZettle website to access daily summaries of transactions, balances, and deposits via a password-protected administrative web page.

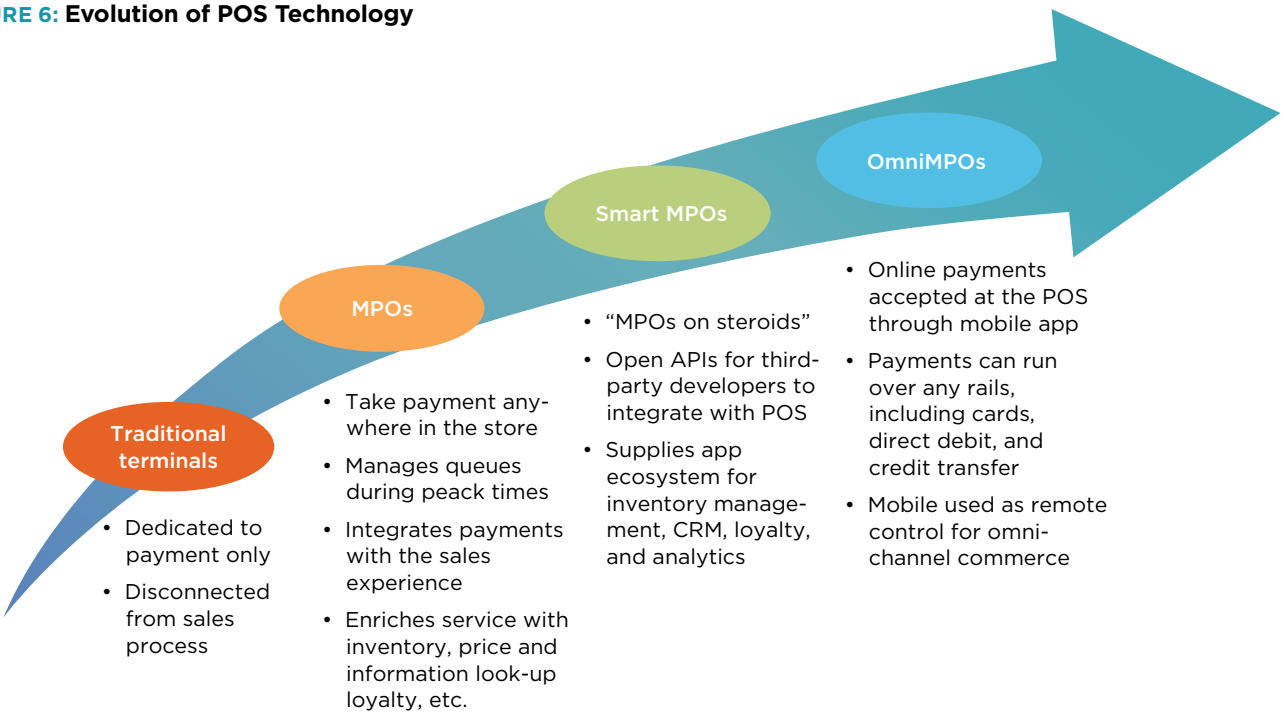
Taxi drivers in India have improved customer satisfaction and increased business opportunities by using an mPOS solution from Spire Payments. Taxi drivers work with Bijlipay (a payment solutions provider) to obtain PosMate, a seat-mounted mPOS device made by Spire Payments. The solution allows passengers to pay by card using a simple interface. It provides security and convenience. As a result, usage has gone up. Passengers frequently come from referrals from international visitors, increasing revenues for taxi drivers.

3.2 MOBILE PAYMENT ACCEPTANCE

The use of mobile phones to transfer mobile money between prepaid e-money accounts, to make deposits, to withdraw funds, or to pay bills continues to expand in emerging markets. Mobile money is largely accepted for the purchase of goods and services at MSMs, and the prospect for further expansion of this type of payment is promising. Payments to merchants can either happen through the typical P2P protocol or follow a special path for a P2M payment. Having a specific P2M type of payment requires the identification of merchants as a special category and possibly a special transaction type. So, while many providers apply a credit-push method for P2M, other providers apply a request-to-pay protocol, where the transaction takes place in two stages. The first stage starts at the merchant with a request to pay sent to the customer, including the transaction value. The second stage takes the form of a credit-push transaction from the customer to the merchant with all information included in the first stage. The customer can either use the USSD protocol to initiate the transaction or use mobile applications that access the prepaid e-money account. USSD provides little flexibility and slow transactions compared to mobile applications.

Achieving interoperability of mobile-payment schemes is critical to the successful evolution of payment acceptance via the mobile channels. Mobile-payment technology is evolving fast, and merchants will greatly benefit from adopting interoperable payment solutions,

FIGURE 6: Evolution of POS Technology



M-Pesa: This service has been successful in many African countries. Vodafone started the service in Kenya, then moved to other countries, including the Democratic Republic of Congo, Egypt, Ghana, India, Lesotho, Mozambique, and Tanzania, sometimes under a different brand name. M-Pesa is a mobile-payment application that manages a prepaid e-money account for each user and provides a bundle of services, including transfers to other mobile accounts, purchases of goods and services at merchants, bill paying, loading from a card or bank account, receiving salaries and wages, receiving international remittances, and much more. M-Pesa had over 37 million active accounts by 2019 and managed over 500 transactions per second in December 2018, totaling more than a billion transactions per month.

PayTM became one of the popular methods of digital payment selected by consumers even at corner kirana stores (mom-and pop stores) in India due to loyalty cashback offers backed by strong advertising. PayTM started as licensed issuers of semiclosed prepaid mobile wallets. The Reserve Bank of India had set a basic monthly limit on these wallets of Re 10,000 (approximately $142) for individuals. The limit could go up to $1,400 if users went through the KYC account-verification process. However, with the introduction of UPI, it was quick to introduce UPI-based payment on the mobile app, enabling account-to-account transfers and doing away with need for KYC of app users.

as opposed to closed-loop solutions. Fast or instant crediting of funds into the merchant account is a major differentiator between mobile-payment acceptance and card acceptance. The merchant is able to reuse the accepted funds to make payments to suppliers immediately. However, to achieve the full benefits of this feature, the entire ecosystem, where suppliers can also accept mobile payments, is required. The identification of merchants as a separate category is important to justify receiving regular funds from different persons (financial integrity) and for the provider to price the service properly, by reducing fees of cash out and to deliver merchant-specific add-on services.

3.3 MERCHANT QR CODE

The QR code is a simple, cost-effective payment-acceptance solution that enables merchants to present their own individual QR codes for consumers to scan and pay using e-wallets. A QR code is formed of a matrix of barcodes that contain merchant-specific details and is displayed by the merchant as a printed placard or in digital format at the point of interaction. It can be an effective solution to enable the inclusion of a wide range of cash-based, previously excluded merchant segments into the financial sector. The solution costs and value proposition are very appealing to MSMs, requiring a bank account, a smartphone, and a designated merchant QR code display.

EMVCo announced a standard for the QR code. The standard recognizes both merchant- and consumer-presented QR code. Consumer-presented code will always be a dynamic QR code issued from the consumer's mobile phone and contain the merchant's information and the amount to be transferred. Merchant-presented mode (MPM) QR code could be static (presented on paper and showing only merchant information) or dynamic (presented on a mobile or computer device and showing both the merchant's information and the amount to be transferred). The merchant would need a mobile phone in all cases to receive payments. The EMV® QR Code Specification for MPM can enable account-based payment as well as card-based payment. This feature increases the interoperability, efficiency, and flexibility of QR code deployments based upon the EMV specification. In addition, The EMV® QR Code Specification for MPM enables multiple different domestic and international payment programs through a single QR code. This flexible approach could be adopted in any marketplace and has the option to enable migration to the globally interoperable EMV framework to widen acceptance internationally.

For the consumer- or payer-presented model, the consumer displays a QR code on a mobile application, typically linked to an e-money or card account. Then the merchant uses a scanner or another mobile device to read the payment information from the consumer-presented QR code and initiates a payment request. For the merchant-presented model, the merchant displays a QR code, and the consumer uses a mobile application to scan the QR code and launch the interaction interface for the merchant and then initiates a payment request.

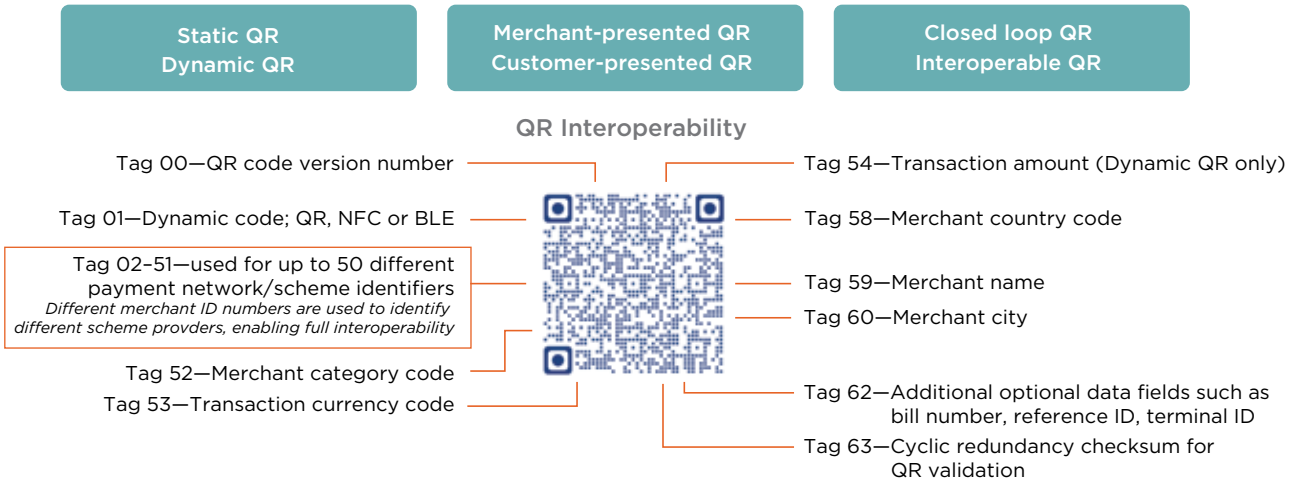
FIGURE 7: QR Code in Comparison with Other Payment Types

	PLASTIC CARDS		QR-BASED PAYMENT			
	Handheld point of sale	Mobile point of sale	Fixed QR	Dynamic QR	NFC/contactless	USSD-based
Cost per transaction	X	X	✓	✓	X	~
Technology requirements	X	~	X	X	~	✓
Terminal cost	X	~	✓	~	~	✓
Distribution complexity	X	X	✓	✓	X	X
User learning curve	✓	✓	✓	✓	✓	X
User experience	~	~	~	✓	✓	X

✓ Positive feature ~ Neutral feature X Negative feature

Source: QR Code and Financial Inclusion (CGAP, 2018).

FIGURE 8: QR Code Characteristics



Source: World Bank Group

In some emerging markets, QR code solutions are supported well by merchant acquirers, payment schemes, and regulators due to their great potential and capacity to transform the payment-acceptance landscape, particularly for MSMs. QR code innovations are also facilitating more effective collaborations among key payment actors in markets, bringing them closer to interoperability. One key issue that many markets are addressing is the interoperability of QR code, so that a merchant with a specific acquirer can accept payments from consumers having their accounts with banks different than the merchant's bank. A key benefit to merchants in having a single QR code is that it includes acceptance of the international payment brands and domestic networks as well as merchant proprietary data. It also supports multiple use cases, such as adding tips and convenience fees, paying bills, and supporting alternate languages.

In India, the introduction of mobile-money wallets, mPOS, and QR codes has contributed to the reduction in the cost of EPA. The merchant-acquisition process has been remarkably revamped by leveraging the Aadhaar digital ID and collaborating with credit bureaus to eliminate heavy-handed paper-based underwriting processes. But the introduction of Bharat QR code by most wallet providers has led to a simpler, cost-effective merchant-acquisition and onboarding process, providing new wider solutions for the challenging last-mile acceptance enablement.

According to the Reserve Bank of India, the Bharat QR code is the world's first interoperable payment-acceptance solution. Bharat QR code standardized the QR code payment method throughout the country. Payment networks such as Mastercard, American Express, and Visa have collaborated with the National Payments Corporation of India to launch and promote the Bharat QR code payment method.

The ability of the Bharat QR code to accept payment from different bank wallets differentiates it from other closed-loop QR code solution providers, which require their customers to install the same branded app and an account on their smartphones to allow payment transactions. Bharat QR codes enable direct bank transfers through the Immediate Payment Service to a bank account and not through email or mobile phone numbers. The merchant setup for a Bharat QR code requires a bank account that links to the Bharat Interface for Money (BHIM) app. The BHIM mobile-payment app was developed by the National Payments Corporation of India and adheres to UPI standards. It generates an individualized merchant QR code that can be printed and displayed for customers to scan and pay. Customers can pay a merchant using their own bank app or the BHIM app and authenticate the payment with a four-digit passcode to generate instant merchant payment. The Bharat QR code solution eliminated the traditional POS terminal cost and the merchant transaction fees paid to the merchant POS service providers.

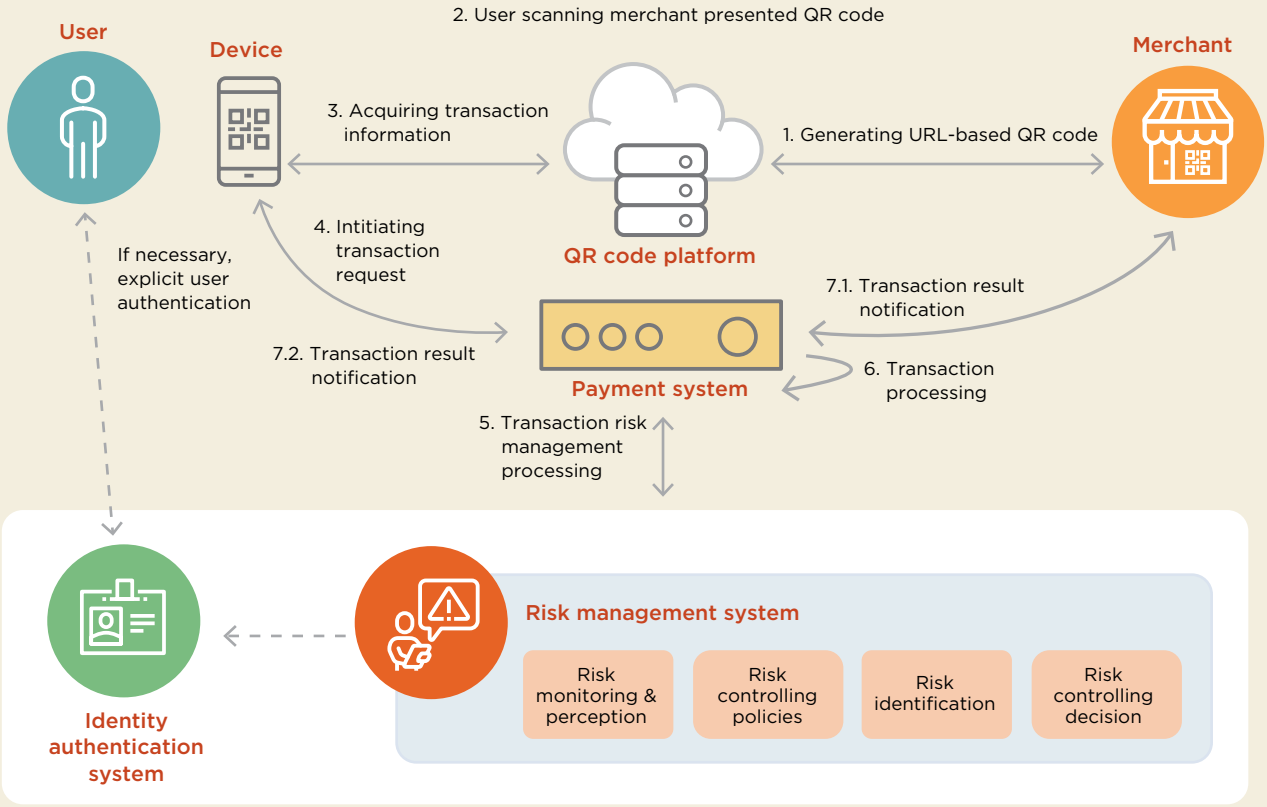
Thailand

In 2017, Thailand introduced Thai QR Payment platform, a standardized and interoperable QR code platform based on the EMV standard that has helped onboard millions of merchants in just a few years, vastly expanding EPA in a market that was reasonably well banked but still saw cash dominating retail payments. It supports an open infrastructure and interoperability, as well as multiple mobile applications and payment instruments (credit and debit cards, bank accounts, and e-wallets), and is available for both domestic and cross-border payments.

Ant Group QR Codes and Security[19]

QR code providers such as AliPay use a number of security measures to ensure transaction safety. Providers avoid including sensitive transaction information and tend to add such information within a trusted QR code platform. In addition, security methods, such as a unique order number, timestamps, a transaction message signature, and sensitive data encryption, are used to ensure transaction security and prevent replay attacks and man-in-the-middle attacks.

Figure 9: Merchant-Presented QR Code Payment Process



3.4 ELECTRONIC WALLET APPLICATIONS

Over the past few years, e-wallet applications have expanded rapidly, offering features that allow consumers to pay and receive payments conveniently. The e-wallet apps enable payment for goods and services from different sources, including a consumer's debit and credit cards, prepaid cards, and bank accounts. The e-wallet is just considered a new channel or form factor to access traditional bank accounts and cards.

Upon paying through a card within an e-wallet, the transaction falls under the network scheme's payment rules, terms, and conditions; the use of mobile is just a new channel to access the card account. The transaction is typically considered a CNP transaction.[20] When using a bank account, either the transaction is performed as an internal transaction within the bank or the Automated Clearing House, real-time gross settlement, a fast payment system, or another domestic interoperable infrastructure is used to make the transfer across banks.

MSMs in emerging markets could benefit from the expansion of e-wallets. Some mobile wallet applications provide access to cards and bank accounts, plus e-money accounts owned by the same individual. For example, the PayPal application requires access to a card and gives the user an option to access an e-money account managed

Venmo: This wallet enables a bank account, credit card, or debit card to be linked to it. Venmo focuses on simplifying payments to and from the user's immediate social circle. Sending money is simple, similar to writing an email, and the app can access the user's entire contact list if the user chooses.

Square: Square wallets offer solutions to customers holding smartphones that are not NFC enabled. The Square e-wallet enables customers to pay at the point of interaction using the merchant's Wi-Fi network. Once the customer is within 100 meters of the merchant's physical checkout point, the customer's phone will appear on the merchant's acceptance device and the customer can self-identify and initiate payment. Square wallets can link loyalty cards for merchants to their own e-wallets to benefit from usage promotions.

PayPal: This wallet lets people pay with a PayPal account, a credit or debit card, a bank account, or a line of "bill me later" credit that can be applied for within the app. PayPal can be used to make a transfer to another person or to a merchant. Like Google Pay Wallet, the new PayPal app incorporates deals and discounts that are then automatically applied when users pay. Users can still send money the traditional PayPal way, but the new app also integrates ordering, couponing, and paying within PayPal's merchant network. PayPal is also entering mobile payment via a card reader with the PayPal Here app.

BHIM: The National Payments Corporation of India developed this interface as part of the Digital India Initiative. Users can access all of their bank accounts in one place, and there is no need to download mobile apps from multiple banks. BHIM is a UPI-based app that enables money transfers using just a mobile number. Other than that, user functionality is similar to UPI, where payments can be made through a virtual payment ID or through an account number and bank/branch code known as the Indian Financial System Code (IFSC).

by PayPal. Examples of mobile wallets include Venmo, Apple Pay, Samsung Pay, Google Pay, PayTM, Orange-Cash, and Vodafone Money.

3.5 MERCHANT NFC ACCEPTANCE

NFC is an upgrade of the existing proximity card standard (radio-frequency identification) that combines the interface of a smartcard and a reader into a single device. It allows users to share content between digital devices, pay bills wirelessly, or even use their mobile phone as an electronic traveling ticket on existing contactless infrastructure already in use for public transportation. Due to its shorter range, NFC provides a higher degree of security than Bluetooth and is suitable for crowded areas, where correlating a signal with its transmitting physical device (and, by extension, its user) might otherwise prove impossible.

To use NFC for making a payment, a mobile wallet app that is linked to a payment card or a bank account needs to be installed on the customer's mobile phone. The merchant can accept payment through NFC-enabled readers/certified terminals when customers hold their cards or phones near the reader device—a simple tap and pay. This is a transition from swipe and pay to dip and pay—both requiring physical cards.

Google Pay, Apple Pay, and Samsung Pay: These pay wallets are e-wallets that use tap-and-pay apps. They store tokens representing the credit- and debit-card information for use in a store and online. Pay wallets use tokenization technology to authenticate transactions. They work only on the operating system associated with their device (for example, iOS for Apple, Android for Google). They can track merchant discounts and add issuer-driven cashback awards to drive usage. These pay wallets have seen tremendous growth around the world due to the convenience provided to users.

After a slow start, the adoption of NFC-based pay wallets (Google Wallet, Apple Pay, Android Pay, PayPal, Samsung Pay, Square Wallet) is gaining traction among consumers globally. Apple Pay alone has close to 250 million users. The uptake in acceptance of pay wallets has been driven by consumers' strong interest in convenience and security, and by cashback incentives provided by some wallet issuers. With technology vendors providing seamless integration of NFC within the mPOS environ-

ment, retailers are now able to provide consumers with more choices for how to pay. Mainly as a result of this, NFC-ready POS terminals are expected to grow at a compound annual growth rate of 17.9 percent, from 45 million units in 2016 to 86.9 million units in 2020.

3.6 UNIFIED PAYMENT ACCEPTANCE SOLUTIONS

In many markets, third-party processors have emerged in the acquiring value chain, offering integrated or unified merchant account services for accepting different types of payments. Such PSPs bundle the payment gateway with the merchant account to offer e-commerce and face-to-face merchants an integrated API-based software solution that allows merchants to accept different payment methods in multiple currencies, including international and regional card brands, digital and mobile wallets, and the Automated Clearing House. The solution also allows merchants to build and customize their payment-acceptance platform based on the needs and spending habits of their customers.

Certain PSPs also allow merchants to customize and add modules that can request payments from customers and set up recurring payments and subscription billing. In addition to payment acceptance, PSPs also provide such other value-add services as fraud protection, account management, and reconciliation tools. Lastly, API toolkits are also available to merchants who want to integrate the payment services with other third-party systems (for example, Shopify) to streamline customer experience. Although POS acceptance is not the core value proposition for unified acceptance solutions, PSPs provide software development kits to integrate the existing POS with a merchant's e-commerce website or mobile app.

3.7 MERCHANT AUDIO QR

Audio QR enables transaction processing between connected devices when they are placed within a suitable range. For a large number of financially excluded people, obtaining access to mobile phones is easier than getting financial access. Audio QR technology is highly applicable in such environments because it makes mobile phones payment ready and acts as a substitute for QR code scanning and NFC payment. Its main benefit is that users need only a basic mobile phone with a speaker and microphone to transmit payments securely. It doesn't require a camera, as a QR code scanner does, and it doesn't require a dedicated chip in the transmitter and receiver, as NFC does.[21] Audio QR uses ultrasonic sound functionality.

Google Tez: In 2018, Google entered the audio QR payment arena by launching Google Tez in India. The app can be used for various purchases online and offline and was created in compliance with India UPI. The transfer of funds between devices is instant, and it requires no bank account details, phone numbers, or other sensitive information to be exchanged. It works simply by placing phones together, requesting a payment, and entering the customer's UPI PIN. As of 2018, Tez had been rebranded as Google Pay. The service is integrated with Uber and a range of retail brands, such as Big Bazaar, e-Zone, and FBB.

3.8 RECOMMENDATIONS

- Solutions such as QR code can greatly accelerate MSM inclusion in the formal financial system. Regulators need to ensure that QR code technology is
  - Available for implementation to domestic and international providers under the same requirements;
  - Interoperable, so merchants associated with one service provider can accept payments from all other providers;
  - Secure, so no sensitive information is transferred between the user or merchant and the associated service provider, and with proper fraud-management aspects built into it; and
  - Supported by mass financial-literacy efforts to promote usage.
- Regulators need to ensure that proper regulations govern the e-money services. Regulations should
  - Allow a level playing field for banks and non-banks as well as domestic and international providers;
  - Ensure that interoperability exists among service providers;
  - Ensure protection of consumer funds; and
  - Ensure that MSMs can receive prices of goods and services in near real time or, at most, before the end of the business day.
- Merchant aggregators, payment facilitators, acquirers, QR code providers, and other PSPs should be subject to proper oversight by the payment system overseer. The oversight of such providers should be proportional to the risks that the PSPs introduce to their customers and the market.

4. Merchant Charge or Fee Types and Options

TYPICAL MODELS

At times, the high costs of merchant acceptance inhibit progress in merchant acquisition. To accept payment cards, merchants have to invest either up front or on a monthly basis for POS terminals; this requires that MSMs make a significant monetary outlay. Additionally, merchants could be liable for paying stiff penalties if they do not meet the minimum volume requirements, transaction chargebacks due to fraud, and a high merchant discount fee (which at times may reach 4 or 5 percent).[22] The merchant fee is an important consideration for MSMs and is usually an inhibitor in terms of growing acceptance. For them, the cost of accepting electronic payment is high in comparison to the low perceived cost associated with cash payment. MSMs feel that cash has no cost, as they receive the full value of each transaction, while during electronic transactions, they have to pay the merchant fee or the merchant discount rate, resulting in a decrease to the net value received by merchant. In many markets, merchants perceive that electronic transactions could also open them up to a tax liability.

4.1 THE FOUR-PARTY MODEL INTERCHANGE STRUCTURE

BOX 1

THE FOUR-PARTY MODEL

Visa, Mastercard, and most domestic card network schemes operate on the basis of a four-party interchange distribution model. In addition to the network scheme, four parties are involved in a transaction: the account holder, merchant, issuing bank, and acquiring bank.

The transaction follows the following steps:

Step 1: The customer purchases goods or services from a merchant using a payment scheme–branded payment card.

Step 2: The payment is authenticated. The merchant POS system captures the customer's account information and securely sends it to the acquirer.

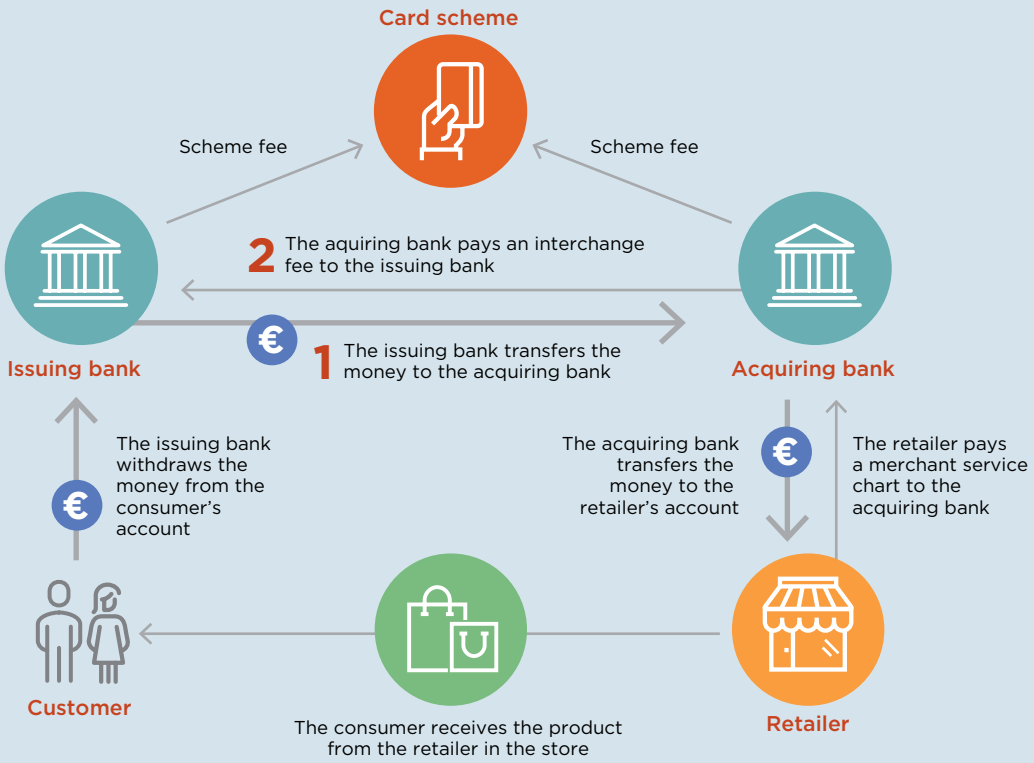
Step 3: The transaction is submitted. The merchant acquirer asks the network scheme to get an authorization from the customer's issuing bank.

Step 4: Authorization is requested. The network scheme submits the transaction to the issuer for authorization.

Step 5: Authorization response. The issuing bank authorizes the transaction and routes the response back to the merchant.

Step 6: Merchant payment. The issuing bank routes the payment to the merchant's acquirer, who deposits the payment into the merchant's account.

Figure 10: Typical Four-Party Model Interchange Fee Distribution



Source: 2016 European Commission Regulation on Interchange.

4.2 THE THREE-PARTY MODEL

In a three-party model, the issuer and acquirer are the same entity. As both the relationship with the merchant and cardholder are established directly with the payment network, there is no interchange fee and no charges to be exchanged between the two parties. The revenues associated with this model are much more profitable for the network. Examples of three-party networks include American Express and Discover, which in certain markets have adopted the four-party model by outsourcing or franchising services to issuers and acquirers to enhance their customer reach and revenues and to compete better in the marketplace.

Based on the brand of the card used by the cardholder, and based on the accepted brands by the merchant, the transaction can follow either the four-party or three-party model, including the rules and fees of the scheme.

4.3 MERCHANT FEE TYPES

This section provides a detailed example of how the fee structure works for the four-party model. This pricing model applies only to payment cards and is not applicable to mobile-money solutions; mobile-money fees will be addressed in section ↑ 4.6. Merchant fees are the fees charged by the merchant acquirer or the processor to the merchant for processing payment-card transactions and providing merchant services. The most significant component of these fees is the merchant discount fee that is applied to every processed transaction. Additional merchant fees may be incurred by the merchant, depending upon the market and the merchant agreement terms and conditions. These include terminal fees associated with its price or rental, cross-border fees, and chargeback fees.

The merchant discount fee—also known as the merchant service fee, merchant service charge, or merchant discount rate—is the fee paid by the merchant to its acquirer bank or the contracted party for services related to the processing of the merchant's card transactions. In the four-party model, merchant fees typically fall into two categories: wholesale fees and markup fees. ***Wholesale fees*** are paid by the acquirer to the issuer (***interchange fees***) and to the card scheme (***assessment fees***). ***Markup fees*** are paid by the merchant to the acquirer. In a three-party model, there are no interchange fees, but the merchant is charged a merchant discount fee on each transaction for merchant-acquiring services.

4.3.1 Interchange Fees

The interchange fee is a percentage of the transaction that is paid by the acquirer to the issuer. It exists only when the issuer is a different organization from the acquirer. For a POS transaction, the interchange transfers funds from the acquirer to the issuer to compensate the issuer for costs incurred to provide the guarantee (fraud and credit losses), prompt funding (float), and selected processing costs where the revenue for these costs is collected via the merchant discount rate. Card schemes develop interchange fee schedules at a country, regional, and interregional level. Interchange fees can vary based on card product type (credit, debit), card features (silver, gold, platinum, and so forth), merchant category (retail store, hotel, government, and so on), processing type (card present, card not present), transaction size (small transactions), and other factors. Interchange fees are applied per transaction and typically take the form of a percentage of the transaction plus a fixed value, such as 1.1 percent plus $0.10 or only a percentage (credit or debit) or fixed amount (debit).

4.3.2 Other Fees

Assessment fees are charged by the card network and charged per transaction on a per-transaction basis split between processing (fixed) and brand (percentage of amount). Acquirers include a markup of their costs in the merchant discount rate charged to the merchant. The markup or acquirer fees are charges by the acquirer to cover its expenses, risks, and chargebacks, and finally as a revenue stream for the acquirer. Other fees could be applicable at certain conditions, such as merchant rental and maintenance fees, which cover monthly rental and maintenance charges for POS terminals that are sometimes absorbed by the acquirer bank or service provider; merchant cross-border transaction fees, which are charged to the merchant when a customer uses a card from an issuing bank not located in the same country as the merchant's processing account; and merchant chargeback fees, which are applied by the acquiring bank to cover the costs of investigating disputed and fraudulent transactions.

4.4 OFF-US VERSUS ON-US PRICING

An off-us transaction occurs when the acquiring bank and issuing bank are two different legal entities, and the regular interchange flow rules apply. Off-us is a more common type of a transaction, as there are typically more issuers than acquirers in a market.

On-us transactions occur when both the issuer and the acquirer belong to the same legal entity. If both the issuer and the acquirer belong to the same bank, there is no need to go to the card network to seek and obtain the authorization and validation on funds for the transactions.

BOX 2

AN EXAMPLE OF HOW THE FEE STRUCTURE WORKS IN A FOUR-PARTY MODEL

In this example, a branded credit card is used to purchase $100 of goods from an online retailer.

- The pricing for online transactions is 1.99 percent plus $0.25 per transaction.
- For the $100 transaction, the merchant will receive the following amount:
  - Transaction value: $100
  - The acquirer takes $2.24 (1.99 percent plus $0.25). This is the merchant discount fee.
  - The merchant receives $97.76 from the acquirer.
- This $2.24 is distributed to all participants in the value chain as follows:
  - Since this is a CNP (online or e-commerce) transaction, the fraud risks are high. The issuer gets the CNP interchange rate, which covers investments made to mitigate fraud risks and so forth.
  - Based on criteria for online payments and card type, the card issuer is entitled to 1.65 percent plus $0.15, or $1.80. This is the interchange fee collected by the acquirer.
  - Note: The issuer gets the maximum amount in a four-party model due to investments made to cover the fraud and credit risks and marketing costs incurred encouraging cardholders to use electronic payment.
  - So the acquirer receives $98.20 ($100 – $1.80) from the issuer.
  - The merchant gets $97.76 of that money. (The merchant discount fee was $2.24.)
  - The remaining $0.44 is used by the acquirer to pay its costs and margin.
  - The payment network's assessment fee is assumed to be 0.10 percent, so they get 10 basis points ($0.10) of the transaction value of $100.
  - The acquirer gets the remaining $0.34. This amount may be split with other players (for example, payment facilitators, processors, and so on) if the acquirer has outsourced some of the activities.

An on-us transaction is more beneficial for banks, as they obtain higher transaction revenues from the acquiring and issuing side of the business while reversing little to no revenue back to the network. For on-us transactions, the acquirer bank does not have to pay interchange or network fees. Hence, it can offer better merchant service fees to the merchant upon accepting cards issued by the acquirer bank. This practice is common in some countries, especially where interchange fees are unreasonably high. As a result, merchants in these countries end up having a number of POS terminals, each belonging to a different bank, and each terminal accommodates a card issued by the acquirer bank. Hence, the merchants avoid high off-us fees and benefit from low on-us fees. This practice may be beneficial to financial institutions but harmful to the market, as it is cumbersome for the merchants (who must maintain separate terminals and separate bank accounts for the payments through each terminal), replicates infrastructure, avoids interoperability, minimizes the profitability of acquirer banks, and limits the business relationship between merchants and acquirer banks.

NEW MODELS

4.5 PRICING MODELS

The merchant discount fee can have a number of forms:

a. Interchange-plus, where the merchant pays the wholesale plus an agreed-upon markup to the acquirer bank per transaction. This is the most common form used with merchants.

b. Subscription/membership, where the merchant pays wholesale plus a constant monthly membership fee. This model is very useful for merchants who have a large number of transactions.

c. Flat rate, where all transactions are subject to a certain percentage fee (for example, 2.5 percent), regardless of the transaction size, card type, or any other factor. A flat rate is easier for merchants to read but tends to be more expensive and less transparent. For merchants whose transactions are of very small value, it may be a cost-effective option.

d. Tiered, where transactions are categorized into qualified transactions with lower fees based on such preset criteria as card-present and same-day assessment, and mid-qualified or not-qualified transactions, with higher fees.

4.5.1 Flat-Fee Merchant Models

For some merchants, the sophistication required to calculate the merchant fees is a big obstacle in accepting e-payment. PayClip in Mexico launched an innovative mPOS solution to encourage non-cash usage by targeting 25 percent of the 5.1 million merchants that did not accept cards as their potential customers. The service was open to enrollment for both merchants and individuals, and the recruitment process was a simple five-minute questionnaire to gather relevant data points. Qualified customers received a mobile Clip reader (dongle) free of charge. The Clip reader operated on both Android and iPhone devices with a downloadable Clip app. Clip charged the same flat rate for Visa, for Mastercard credit and debit cards, and for American Express transactions. Although the average merchant discount rate (3.6 percent) is higher than the prevailing rates for large merchants in Mexico, the model is still attractive to MSMs due to the simple and transparent calculations for some merchants. PayClip's flat rate, free Clip reader, easy enrollment, and mobile phone–based application process created a good value proposition for both consumers and merchants.

4.5.2 Merchant Small-Ticket-Transactions Interchange Fee (Payment Schemes)

To promote acceptance of electronic payment in the MSM segment, Visa and Mastercard introduced a lower interchange fee for small-ticket-value transactions between $10 and $15. They also defined the list of merchant categories that could benefit from the special pricing model. The rationale behind the lower interchange fee is to create the right balance to incentivize card use and acceptance by MSMs and to improve the transaction-acceptance economics for MSMs. Additionally, with global volumes of cash usage at MSM retailers standing at around $19 billion, this segment provides a massive untapped opportunity for the payment networks to grow electronic payment.[23]

This small ticket interchange fee structure is applicable for fast food, taxis, parking lots, video rentals, convenience stores, theaters, newsstands, car washes, copy centers, laundry services, and bus lines. The applicability of the special merchant interchange rates for small transactions for the international card schemes may vary by market and in accordance with merchants' individual pricing agreements with their acquirers. The agreements may include other services provided by the acquirer, for which different charges apply.

4.5.3 Installment Payments

Installment payments are also referred to as installment lending or installment credit. At the basic level, installment payments are transactions that are split into a series of payments that a consumer pays over time, rather than paying one lump-sum amount at the time of purchase. An installment payment is a fixed amount of money that the consumer borrows; then the consumer makes specific monthly payments until the loan is paid off. The loan will have an interest rate, repayment terms, and fees, which will affect how much the consumer pays per month.

A number of credit card issuers offer qualifying consumers installment loans as part of the credit card product portfolio. Two well-known industry examples of installment payments are American Express' "Pay It Plan It" feature and Chase's "My Chase Plan." Both products allow end-to-end digital fulfillment, where the consumer can go on the issuer-provided app or online account to select qualifying purchase transactions that have already been made (typically over $100) for fixed, equal, monthly installment payments. Alternatively, consumers can also calculate plan options before a purchase is made.

Several fintech companies (for example, Afterpay and Klarna) provide intermediary services to merchants and e-commerce sites to offer installment loans directly to consumers.[24] Many merchants employ this strategy to increase the ticket amount or number of orders or to encourage repeat customers. A consumer can select a qualifying product (based on ticket size) and select the payment options, including a fixed fee and payment terms. Customer credentials reside with the installment payment provider (intermediary), and those credentials can be used across many merchants.

Under either scenario, whether issuer or intermediary managed, the merchant is paid the total amount of the product at the time of purchase even though the customer is paying in installments. The installment payment provider assumes the risk should the consumer default on a payment. The risk premium is built into a fixed fee per transaction or may even be charged as a percentage fee of the total order amount.

4.5.4 Convenience Fees

A convenience fee is a fee charged to a consumer, rather than the merchant, when a payment card is used for the purchase. Convenience fees can be a fixed amount or a percentage of the transaction amount, usually around 2 or 3 percent, and must be disclosed to the consumer in advance. Types of payments where the payee typically charges a convenience fee include mortgage payments, gas stations, government services, college tuition, and taxes. In many markets, the government could be reluctant, due to existing laws or regulations, to cut part of its

service fees to accept electronic payments; hence, convenience fees could be an option to allow government units to accept payments through cards or any other electronic payment instrument. Convenience fees are set by the network and agreed upon by participants within the market. It should be noted that a convenience fee is different from a surcharge, which is a charge for simply using a payment card. Surcharges are illegal in many countries. All businesses have to follow the policies of payment processing providers and government laws when it comes to convenience fees and surcharges.

4.6 FEES FOR MOBILE TRANSACTIONS (USER OR MERCHANT)

Mobile-money solutions continue to grow and evolve globally due to the introduction of flexible pricing arrangements and the timely adoption of best practices from other markets. One such model that is now being applied by mobile-money service providers is the dynamic pricing model. The model has significant benefits in supporting the different stages of market development, as it enables the service provider to amend prices to respond to shifts in the market; influence or correct end users' unfavorable usage practices to safeguard against unintended service use; and protect against revenue leakages due to users' malpractices.

The dynamics of mobile-money markets are different from those of the four-party models. At the early stages of market development and especially in new markets, the focus of card schemes is to issue cards to develop a large customer base, so there is a need to incentivize the issuer banks to issue and service more cards and, hence, a need to fund the process mostly through interchange fees. The dynamics of mobile money is geared more toward P2P and bill-payment use cases, where the payer pays the transaction fees. While P2M was not one of the early use cases in the mobile-money ecosystem, there was no huge dependence on merchants to cover the costs of attracting new users to mobile-money services.

In mobile-money transactions where the user and merchant belong to the same service provider, mobile-money operators may not differentiate between P2M and P2P transactions and may apply the fee structure of a P2P transfer (that is, paid by the user). In other schemes, they consider a special fee for P2M transfer, paid by the merchant. Considering that P2M is a strong driver for the expansion of mobile-money transfers, the merchant fee can be reduced or even waived to encourage circulation of money within the network. However, in interoperable platforms, where the user and merchant belong to two different operators, the dynamics of the transaction need to be studied carefully.

It is worth noting that many merchants within mobile-money schemes act as agents. In the case of the merchant having a single pool of funds for both roles, it will be in the best interest of the merchant to achieve the greatest possible turnover of such funds. Using e-money for cash-in and cash-out as an agent, accepting e-money from customers as the price of goods and services, and paying e-money to suppliers, the merchant will need to keep a certain balance of e-money. This balance should increase when both the use cases of e-money and the number of customers paying in e-money increase.

4.6.1 Dynamics of Mobile-Money Fee Structures

Consider two mobile-money operators, where user P belongs to network A, and merchant M belongs to network B. A transfer from P to M will incur a cash transfer from P to A and from B to M that will happen instantaneously, while a cash transfer from A to B may happen instantaneously—in case of interbank fast-transfer arrangements—or later within the day—in case of deferred settlement. In the case of immediate settlement, the cost of cash to network B will be zero, and in the case of a deferred net with multiple settlements per day, the cost of cash will be near zero. However, in the case of a next-day settlement or later, the cost of cash could be calculated as a cost element. Another cost element could be the cost of an agent when user P cashed in the fund at his or her account. An argument may be raised that the cost of using the agent at network A might be paid back by network B. A counterargument could be that purchases from merchants are not typically the main driver for the cash-in process, and that the use cases for network A would include transfers to other users and bill payment. Hence, network B shouldn't pay the cash-in fees for network A because the fund was not dedicated to this payment to merchant M. The previous arguments suggest that the only possible fees that may be charged will be processing fees for the interoperability platform, while there is no strong business case for interchange fees in mobile money. However, the interoperability among mobile-money networks will need further study, especially to address agents' interoperability (person to agent and agent to person) and the possible fee structure.

4.6.2 Examples of Mobile Fee Structures[25]

M-Pesa in **Kenya** adopted high prices for money transfers due to its strong competitive market position and weighted its fees higher toward transfers versus cash-out (60:40 ratio). The final cost of a transaction is driven by a staggered pricing table, which directs higher fees to higher transfer amounts.

Mobile-money providers in **Tanzania** followed a different pricing model. They weighted the fee higher toward

withdrawals/cash-out versus transfers (85:15 ratio), which was not the original market pricing structure. Providers in Tanzania shifted the price higher toward cash-out to address growing malpractice by users who avoided transfer fees by depositing funds directly into someone else's mobile-money account. A change in the pricing model to a higher fee for cash-out was a deterrent to such practice.

In **Ghana**, mobile-money service providers leveraged pricing models to encourage customers to reduce their use of over-the-counter transaction services and increase wallet-to-wallet usage. They have achieved this by increasing over-the-counter pricing while reducing wallet-to-wallet transfer costs.

Dynamic pricing models can play an important role in influencing product adoption by customers and can also improve profitability. Mobile service providers in many markets are incentivizing consumers to adopt more wallet-to-wallet services due to their lower cost structures and higher profitability with the prospects of cross-selling additional digital products.

4.6.3 Zero Merchant Acceptance Fee Model

In July 2011, Ant Group officially launched a QR code payment business to provide convenient, efficient, and low-cost payment services for the market. Ant Group's QR code payment solution adopts both customer-presented and merchant-presented models. The merchant fee model is differentiated according to specific payment service types. For the individual-type payee-presented model, it is free of charge. For the payer-presented model and the merchant-type payee-presented model, the merchant service fee is about 0.6 percent of the transaction value. The merchant service fees are discounted to encourage new MSMs to accept electronic payments. Once the transaction is completed, the funds arrive at the merchant's AliPay account in real time and can be used to purchase goods from suppliers immediately. Ant Group cooperates with Alibaba's e-commerce supplier service platform to enable merchants to reach their suppliers from AliPay Wallet. Otherwise, the merchants can also withdraw funds from their AliPay account to their bank account.

The trend of reducing merchant fees is due to different market-specific factors. For example, Safaricom in Kenya reduced its merchant fees from 1.5 percent to 0.5 percent in 2017. In March 2020, in response to COVID-19, M-Pesa waived merchant transaction fees for all transactions below K Sh 1,000. In Malaysia, Mobile Money International enables merchant acceptance on a fee basis of 1.5 percent. In Malaysia, a merchant can be signed up for mobile money with no minimum monthly transactions, no rental fees, and no merchant account. The option of an e-commerce WebLink may also be available to merchants on a fee basis of 2.5 percent. The speed of merchant pay in the WebLink solution is the transaction date plus two days (T+2), and all the required procedures for consumer transaction refunds are in place.

4.7 RECOMMENDATIONS

- The cost of acceptance (in the form of merchant discount rate) can be a disincentive for MSMs to accept electronic payments. The stakeholders need to find the right balance between business sustainability and fee structure for merchants. In general, push-payment technologies using a QR code and other means cost less than pull payments and should be encouraged to grow acceptance in such segments.
- The stakeholders in the electronic-payment value chain should understand the dynamics of interchange fees and the merchant discount rate and review those fees regularly to evaluate their impact on market growth and innovation, including differentiating between credit and debit card fees and proper consideration for costs of chargebacks and fraud risks, different merchant categories, and size of transactions. The objective of stakeholders would be to maximize the number of transactions at merchants, leading to growing profits.
- Consider implementing an issuer-funded acceptance-development fund in partnership with the industry. This approach has been used in some markets to increase merchant acceptance (Indonesia, Malaysia, and Poland are good examples) and is driven by a coalition of issuers and industry partners. An issuer-funded acceptance-development fund requires participating issuers to invest a percentage of transaction revenue (mainly from the interchange fee) into a fund that is managed by a third party to drive various acceptance-growth initiatives that are deemed appropriate for the country and merchant segments. These funds could be tied to a regulator-driven MSM-specific acceptance initiative.
- The mobile-money and e-wallet service providers should focus on growing the value proposition within the ecosystem by giving users more choices to use their e-money or e-wallet applications coupled with the right incentives to use these to grow transaction volumes. Interoperability between service providers can

help achieve these objectives. If customers become frequent users of the e-money or e-wallet applications for different types of payments, this will allow them to maintain digital liquidity as opposed to cashing out immediately.

- Mobile money and e-wallet–based acceptance channels provide a great opportunity for acquiring merchants who have been excluded from previous digitization efforts. Hence, mobile money and e-wallet providers should consider providing micro merchants with financial incentives to shift to EPA, which can be very profitable for the service providers on a longer-term basis.
- The models for onboarding MSMs should allow for full integration of merchants' businesses with their suppliers and customers. Supply chain–focused digitization should provide the right products and incentives as well as seamless integration of technology to enable the smooth flow of funds among all commercial touchpoints within the supply chain.
- For the sake of expanding financial inclusion of MSMs and maximizing the value proposition, banks and service providers should consider providing packages of services—including supply-chain finance, invoicing finance, small business loans, and small-credit-line facilities—besides EPA. The profitability of financial services should be measured on a client or market basis, not a product-per-client basis.
- Pricing models for interoperability of mobile-money users are still evolving, including P2P, P2M, person to agent, agent to person, and others, and there is no global-level consensus on a proper model. Stakeholders need to consider the market dynamics, including short- and long-term commercial objectives, before deciding on the proper pricing model. Differences between cards and mobile-money dynamics should be understood well, and differences among markets should be considered while developing such interoperable pricing models.

5. Merchant Due Diligence

As part of merchants' onboarding process, merchants would be subjected to various due-diligence measures, including anti-money-laundering and combating the financing of terrorism (AML/CFT) obligations required by law or by service provider agreements; consumer data and privacy-protection requirements; and the ability to assess and limit the risks of exposure to fraud. Additionally, they may also be subjected to various measures related to financial due diligence. The focus of this report, however, is on compliance with crime-related due diligence, especially AML/CFT.

5.1 MERCHANT DUE-DILIGENCE MEASURES

Since 1990, the Financial Action Task Force (FATF), the international body responsible for setting global AML/CFT standards, has required countries to maintain rules compelling financial institutions to undertake CDD measures in relation to prospective and current customers. These measures include the following:

i. Customer identification and verification (often referred to in practice as KYC measures)

ii. Establishing beneficial ownership

iii. Establishing, understanding, and, as appropriate, obtaining information on the purpose and intended nature of the business relationship

iv. Conducting ongoing due diligence, including monitoring the customer's transactions to identify suspicious and other reportable transactions

Such due-diligence measures also need to be undertaken in relation to agents of financial service providers and counterparts that may introduce the risk of money laundering or terrorist financing to the financial services provider. When these measures are applied to merchants for purposes of their inclusion in the payment system, this discussion refers to these measures as merchant due diligence (MDD).

In the past, the nature and scope of due-diligence measures were determined by regulations and industry practices. More recently, and especially since FATF introduced a mandatory risk-based approach to AML/CFT, financial institutions have been adopting proportional CDD measures that respond to the risks of different types of customers, services, and geographies. This approach should also inform MDD, and a brief overview of the key CDD principles are therefore helpful.

5.2 RISK-BASED APPROACH TO CDD

In terms of developing a risk-based approach to CDD at the country level, the country's AML/CFT framework must draw information from a proper national assessment of money-laundering and terrorist-financing risks in the jurisdiction. This assessment informs national policies, laws, and regulations to mitigate the identified risks. When an assessment provides evidence of a low risk of money laundering and terrorist financing, FATF allows leeway.

Countries may elect not to apply AML/CFT obligations when a natural or legal person carries out a financial activity on an occasional or very limited basis (having regard to quantitative and absolute criteria), relative to the person's other primary business activities. Countries may also do so when the risk of money laundering and terrorist financing is low; this occurs in strictly limited and justified circumstances, and it relates to a particular type of financial institution or activity.

Banks and non-bank financial institutions are similarly required to undertake institutional assessments of the money-laundering and terrorist-financing risks associated with their products, customers, and channels. Where FATF standards require or evidence is found of higher risk, enhanced due-diligence measures must be employed. For financial institutions, this could entail the collection of more customer information; extensive and more frequent verification of customer data; enhanced monitoring of transactions; and the adoption of other measures appropriate to mitigate the higher level of risk.

Mexico's Verification Exemption for Low-Value Accounts

After conducting a thorough national risk assessment, Mexico identified criteria for specific low-value accounts to advance financial inclusion. These accounts were seen as appropriate for exemption from the general requirements for the verification of customer identity. Banks were given the option to decide whether such customers need to be verified if the products were subject to appropriate controls and restrictions to ensure that they process only small, low-value transactions.[26] The exemption attracted no negative comments in Mexico's 2018 mutual evaluation for compliance with FATF standards.[27] Countries with appropriate national risk assessments may consider similar exemptions in relation to restricted, limited payment products for micro merchants.

Where the institutional assessments identify risks as lower, institutions may be allowed by domestic law to employ simplified due-diligence measures.[28] Importantly, for the purposes of this report, the FATF recommendations recognized as a potential example of lower risk "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes."[29] These products or services would include payment services designed to support national financial-inclusion objectives.

Simplified due diligence should be commensurate with the lower-risk factors and may include such measures as the following:[30]

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (for example, if account transactions rise above a defined monetary threshold)
- Reducing the frequency of customer-identification updates
- Reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established
- Using agents to identify or verify customer identity

Institutions are also required to ascertain whether any senior domestic or foreign politicians or officials are involved in the business relationship or control the customer. This is highly unlikely in the case of small businesses. In most cases, it may suffice to ask the customer whether any such persons are involved in the business relationship. Simplified measures, however, are unacceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios, prescribed by FATF, apply.[31]

Simplified MDD that mirrors these simplified CDD processes can support efforts to enroll MSMs. In many cases, however, banks implement overly conservative measures that are inappropriate for MSMs operating mainly in the cash economy, thereby complicating or even preventing their enrollment. The application of the following principles may help apply proportionate and tier-based MDD.

5.3 PRINCIPLES TO ENSURE APPROPRIATE MDD

To conduct appropriate MDD, the following principles can provide high-level guidance for identifying the risks of money laundering, terrorist financing, and fraud posed by merchants, ranging from large sophisticated companies to small sole proprietors and from higher-risk to lower-risk businesses:

- Undertake a risk assessment
- Design appropriate due-diligence measures
- Be reasonable and pragmatic about identity verification
- Take reasonable steps to identify beneficial ownership
- Collect contact particulars
- Collect profiling information
- Be pragmatic to include micro merchants

A detailed explanation of how to apply those principles is provided in appendix A.

5.4 SUGGESTED MODEL FOR MERCHANT SIMPLIFIED DUE DILIGENCE

A possible way to implement these principles is by using a tier-based MDD process that lays out specific requirements in relation to different levels of money-laundering and terrorist-financing risks.

In applying the tier-based approach, an important policy consideration is whether the tiers should commence with an exemption that financial institutions may use where merchant risk is low and the product or service is subject to appropriate control measures—for example, very low transactions limits and usage limits.

To develop a tier-based system, it is important to provide guidance not only for merchants ranging from higher to lower risk but also for merchants that range from established enterprises to micro merchants. The tiered framework should link with institutional assessments where financial institutions have assessed the risks of different types and categories of merchants in different regions. (See box in the appendix A.)

The tiered framework would then be linked to the MDD measures in relation to higher- and lower-risk merchants depending on the sophistication of the business enterprise, providing more extensive due diligence in relation to higher-risk businesses (for example, established enterprises with large money flows) than lower-risk micro merchants.

Not all small businesses pose a low risk, but their risk levels can be mitigated by the tiered framework by restricting the type and value of transactions that they are allowed to conduct.[32] Restrictions can be imposed on the number of transactions that they are allowed to perform daily, weekly, and monthly, combined with transaction-value caps—for example, only for transactions less than $20, or a value reasonable to the type of business. The tiered system should also allow for a business to provide more services to its customers when it clears a more extensive due-diligence protocol. This approach allows small businesses to access the payment system while also encouraging them to formalize when their payment-service business needs to grow.

Box 3 suggests some simplified measures for the identification and verification of MSMs. It should be considered based on the jurisdiction circumstances and the associated AML/CFT risks.

It is important to reiterate that FATF is not prescriptive about the particulars to be collected or the methods of verification. What needs to be collected to identify and verify a business will differ from business to business, and the type of verification that can reasonably be undertaken will also differ. Where it is impossible to verify information, risks can be mitigated by capping and restricting the types or value of transactions that can be undertaken.

5.5 SIMPLIFIED WAYS TO REGISTER MERCHANTS

While it is important to ensure that MDD is risk based and pragmatic, it is also important to ensure that enrollment is not unnecessarily complex and does not require merchants to travel far just to enroll in the payment scheme.

5.5.1. Using Facilitators

Payment schemes such as Visa and Mastercard allow small e-commerce and brick-and-mortar merchants to be aggregated as submerchants under a (master) payment facilitator. The payment facilitator aggregates all necessary merchant identification data and sends this to the acquiring bank. In terms of scheme rules for payment facilitators, they are generally responsible for verifying that a submerchant is a bona fide business operation and for monitoring the transactions of submerchants to prevent and detect criminal activity. The acquiring bank generally remains responsible for legal compliance with scheme rules by the facilitator and submerchants.

5.5.2 Using Agents

The use of agents to perform CDD is a well-established process for mobile-money programs. Agents are equipped to collect identification particulars of prospective customers and to view and take photographs of the verification documentation and send these to the service provider for processing and customer approval. Similar processes can be used to enroll MSMs.

BOX 3

SUGGESTED MODEL FOR SIMPLIFIED MDD

Identify the Customer and Verify the Identity	
In the case of a ***micro merchant with a sole proprietor***	**An identification** of the natural person owning the business could be performed and the following information could be collected: business name, type of business, and business address.
	Verification can be performed through the following steps: check owner **identity** against the owner's national ID document or data; **verify** business existence against business license or permit (if any is required); confirm the business's existence by a trusted party—for example, a religious leader or public servant who is a customer—or visit the premises either physically or virtually via photographs or video.
In the case of a ***legal person, partnership, trust, or similar arrangement***	**Identification** can be performed by collecting such information as business name, legal form, proof of existence, and business address.
	Verification can be performed by collecting such documents as the certificate of incorporation, a partnership agreement, a deed of trust, or a similar founding document or evidence of establishment.
Identify and Take Reasonable Steps to Verify Beneficial Ownership (Owners or Controllers of the Business)	
In the case of a ***micro merchant with a sole proprietor***	The **identification** will be for the natural person owning the business, as he or she would normally be the beneficial owner.
	Within the **verification** process, where the owner is the sole beneficial owner, the details were already **verified** above.
In the case of a ***legal person, partnership, trust, or similar arrangement***	Obtain the **identity** of legal persons, those who own or control the business (if any), or, if they cannot be **identified,** the person who is the senior managing official.
	Verification can be performed by comparison with information in the founding documents, public registers, and so on, or by **verifying the identity** of the senior managing official as a natural person.
Identify Who Has the Power and Authority	
In the case of a ***micro merchant with a sole proprietor***	The natural person owning the business would normally hold all authority or may delegate some of it to employees.
	A statement by the business owner provides the best evidence for such a business.
In the case of a ***legal person, partnership, trust, or similar arrangement***	There will be a need to **identify** the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having senior management positions in the legal person or arrangement—for example, senior managing directors in a company or trustee(s) of a trust.
	Such information needs to be **verified** by collecting the memorandum and articles of association of a company, the partnership and trust agreement, the letterhead used, a business website that publishes the names of directors and senior managers, and so forth.
Collect Contact Particulars	
For a ***micro merchant with a sole proprietor***	The owner's residential address and mobile phone number may be the most relevant contact details.
	They can be **verified** through a call or SMS requiring a response sent to the mobile number, or by means of a photograph of the business taken with geolocation data.
In the case of a ***legal person, partnership, trust, or a similar arrangement***	The following information should be **identified:** the address of the registered office and, if different, a principal place of business; a telephone number; and a website address.
	The information can be **verified** by calling the mobile phone number, sending an SMS requiring a response, or visiting the website.

Pakistan: Regulations for Digital Onboarding of Merchants[33]

Minimum Requirements for Merchant Due Diligence
Banks/MFBs shall adopt following minimum due diligence requirement for merchants at the time of onboarding:

Identity Information to be collected
Banks/MFBs shall collect following information in manual or digital form from merchants at the time of account opening:

i. Name of the merchant
ii. Valid CNIC[34] number of the merchant
iii. Mobile number of the merchant
iv. Any other two information fields that are not present on CNIC such as place of birth and mother's maiden name etc.
v. Address
vi. Merchant Type (by Profession)
vii. Expected per month turnover

Documents Required
Banks/MFBs shall collect following documents in manual or digital form from merchants:

i. Electronic copy of front and back side of CNIC
ii. Live picture or Digital photo
iii. Any other document(s), if deemed appropriate

Account Activation
Banks/MFBs shall activate Merchant Accounts after fulfilling following KYC/CDD requirements of merchant:

i. Perform Biometric Verification or Verisys from NADRA.[35] In case of NADRA Verisys, Biometric Verification shall be mandatory at the time of first cash out or within three months of opening of these accounts, whichever is earlier. These accounts shall be deactivated if Biometric Verification is not carried out within three months of opening of accounts.
ii. Ensure Pre-screening of merchants' particulars against lists of entities and individuals designated[36]
iii. Conduct Call Back Confirmation or generate One-Time Password (OTP) for verification from merchants.
iv. Carry out full or Enhanced Due Diligence of merchant as per Banks/MFBs own risk assessment, in light of applicable laws and regulations (if applicable).
v. Acceptance of terms and conditions of account provided in English and/or Urdu language by the merchant.

Account Opening Points

a) Banks/MFBs may offer opening of these merchant accounts at digital touch points such as mobile applications/web portals/ATMs/digital kiosk etc. and at bank branches/Branchless Banking Agents, etc. Further, Banks/MFBs permanent staff may visit merchant place for opening of these accounts.

5.5.3 Using Mobile Phones

In countries where SIM cards of mobile phones must be registered to the user through an adequate KYC measures, the phone itself provides some proof of identity of the user. The link between the handset, number, and user can be strengthened by sending a verification code or SMS request requiring a response by the user. In this approach, the financial institution is dependent on the CDD process that has been performed by a third party, in this case a mobile network operator.

These alternate methods for conducting KYC requirements (for example, the practice of using of SIM registration data for mobile-money KYC in Ghana, Haiti, and Pakistan) remain a very important element of digital enrollment in many countries.

5.6 eKYC AND CENTRALIZED KYC

If universal, national, or digital ID systems are available, then simple and streamlined electronic know-your-customer (eKYC) procedures can be established, and innovation around eKYC can be encouraged to include the following:

- Linkage to national ID
- Acceptance of scanned ID documentation
- Transfer of eKYC data ownership and usage to customer
- Innovation around remote eKYC capture, verification, and adoption

An increasing number of countries are adopting biometric national ID programs that collect data such as iris scans, full fingerprint scans, and photographs supporting facial-recognition software. When service providers are allowed secure and appropriately limited access to such data for CDD purposes, CDD processes will become more effective, secure, and painless for all parties.

5.7 RECOMMENDATIONS

- Authorities should develop guidelines for simplified due diligence covering both individuals and MSMs. Guidelines for simplified due diligence should be developed in the context of the national policy objective of promoting financial inclusion while considering the high risks of excluding a large percentage of the society from financial services and letting a large percentage of transactions (cash) go unseen and unmonitored by the authorities.
- Simplified due diligence may need to identify cases in which delayed verification provisions could be considered through setting transaction or account limits, and conditions where a digital copy of the identification document could be accepted temporarily until the originals are verified in due course.
- Guidelines for simplified due diligence should consider minimizing identification and verification requirements for micro merchants with sole proprietors.
- Guidelines for simplified due diligence should consider using agents for the KYC process, and they should consider remote KYC whenever possible.
- Service providers should consider categorizing merchants with similar activities, business sizes, and geographical locations and develop risk profiles for such categories to simplify the requirements and automate the registration process.

India provides a good example of a national ID program that is used for eKYC purposes. India's Aadhaar National ID Program provides a unique biometric identifier for more than 1.1 billion people in India. The UIDAI, the authority responsible for Aadhaar, has made an eKYC service available to facilitate customer identification. With customer consent and a fingerprint scan, a financial service provider can access the Aadhaar data to verify the client's identity. When the identity of a prospective client is verified, the account-opening form is automatically populated with the client's Aadhaar-registered biographical data. The financial service provider is then allowed to treat that data as sufficiently verified, thereby relieving the verification burden. While the Supreme Court of India has restricted the use of eKYC for general purposes, pending an improved legal basis for such use, banks are still allowed to use eKYC to identify recipients of government subsidies and welfare schemes.

India has also launched a centralized KYC registry. All financial service providers that undertake CDD must submit prescribed customer data to a central registry where all providers are able to access it, thereby preventing the need for multiple duplicative identity-verification processes relating to the same person.

6. Merchant Underwriting Process

TYPICAL MODELS

6.1 FACTORS AFFECTING MERCHANT UNDERWRITING

Merchant underwriting means the evaluation of merchant creditworthiness. The process is typically required by acquirers to evaluate the credit risks of the merchant and the ability to pay for chargeback requirements when the customer returns the goods, the goods are not delivered or damaged, or in cases of frauds or exposures where the merchant is liable. The process is a critical initial step in the merchant-acquisition journey and one of the major challenges for MSMs, since they lack the credit history required to establish their creditworthiness.[37] Several factors affect the merchant underwriting process, and the risk factors associated with the underwriting process may be similar to those evaluated for extension of credit.

The risk underwriters evaluate business owners within specific parameters in an effort to expedite the risk-evaluation processes, focusing on risk-related red flags. The business type is one important indicator of the potential risk level of a merchant.[38] Other key parameters may include previous merchant affiliations and chargeback processing ratios. Other key parameters utilized for the evaluation of new merchants (especially for mid- to large-sized merchants with substantial transaction volumes) are a history of litigation, negative press, or any other unfavorable poor business practices.[39] However, the extent of underwriting requirements should be in proportion to the risks the merchant poses; the underwriting entity may not always apply these risks consistently and adequately.

Acquiring e-commerce merchants is an area of potential risk for underwriting. Regularly monitoring and reviewing merchant activity is critical for e-commerce merchants, as some merchants may observe noncompliant practices to establish new websites or sell new products without informing their acquirer. This represents a noncompliant aggregation and a risk concern in the form of payment fraud.[40] Service-delivery processes in which a merchant invoices and bills the customer in advance of the customer receiving the services, such as event tickets or advance travel booking, and recurring payments, such as registered services, may also represent high-risk factors.

Adoption of credit-push payments (customer-initiated) versus credit-pull payments (merchant-initiated), the migration from magstripe payments to chip and PIN, and the usage of CNP secured payment approaches such as 3D Secure (Three-Domain Secure) are other key considerations, as these are more secure methods of payment and reduce the liability for the merchant in the event of fraud. A merchant's credit history, AML checks, and any previous credit capacity or bankruptcy concerns, together with the merchant's financial standing in terms of owning assets, bank accounts or capital holdings, or ownership of the business, will be other important factors. As a

coverage for credit risks, acquirers ask the merchants to reserve some funds to cover the merchant's obligations in cases of chargebacks of frauds liable to the merchant. The merchant's reserves are evaluated by the acquirer in proportion to, among other factors, the size of transactions, business risks, and average cashback and fraud cases.

6.1.1 Merchant Underwriting Approval Parameters

Approval parameters are deployed to contain and limit merchant transaction risks to the acquirer service provider. The merchant's processing limits are determined by the acquirer as an outcome of the underwriting review conducted by the acquirer. The merchant's processing limits are set in accordance with the merchant's risk level. The merchant's monthly volumes should correspond with the set processing limits and the average transaction values. Large out-of-pattern processed transactions, higher than the merchant's processing limits, may result in the acquirer holding back payment deposits from the merchant's account to validate and ensure legitimacy and the absence of any potential chargebacks.

6.2 REQUIRED DOCUMENTATION FOR MERCHANT UNDERWRITING

The underwriting documentation required by an acquiring service provider includes pertinent details on the merchant's profile to enable a complete risk assessment. Examples of the information collected may include but is not limited to type of business, commercial registrations, legal and operating name(s), confirmation of the address of the place of business, ownership structure, financial standing, bank statements, tax returns, background checks, and credit bureau evaluations on owners, to determine previous risks.[41]

NEW MODELS

Credit-risk assessment is an integral part of the merchant-acquisition process that requires careful and detailed handling to avoid future implications for the business operations and profitability of the acquirer. The quality of the data and the level of market development can make this process time consuming in certain markets, leading to dissatisfaction among new merchants. The major obstacle for the underwriting process is a lack of credit history for most MSMs or the unavailability of alternate credit-scoring models leading to the disqualification of most of those merchants during the credit-evaluation process.

To overcome these obstacles, new models for merchant acquisition are gaining momentum in many countries; new market entrants are establishing new standards for the turnaround time in merchant onboarding. *Most of the models covered in the following section use a process for underwriting similar to those used by lenders when evaluating credit before granting business loans.*

6.3 ALTERNATE DATA SOURCES

Innovations in underwriting-automation software are also speeding the identification of critical elements of merchant risk, enhancing decision-making processes surrounding merchant risk, expediting merchant onboarding time, and improving the overall productivity of risk underwriters.[42] Innovations in the use of cloud-based alternate data sources and evaluation models are also allowing for better evaluation results for acquirers. In a recent study, *New Credit-Risk Models for the Unbanked*,[43] McKinsey and Company identify six different sources of overlooked data that can be useful for creating an alternate credit-scoring model: (i) telecommunication providers, (ii) utilities, (iii) wholesale suppliers, (iv) retailers, (v) the government, and (vi) financial institutions. Other alternate data sources may extend to social media (LinkedIn and Facebook) and user behavior on the website during registration.

6.3.1 Mobile Network Data

Mobile network data can be very useful in developing a model for creditworthiness. Data elements that can serve as indicators of business performance include the number of calls and text messages received during working hours, location during working and non-working hours, regularity of payments, including prepaid payments, patterns of voice versus internet usage, and even writing a family name rather than a given name. In their normal operations, mobile network operators gain detailed information about customers' usage, locations, and regularity of payments. If accompanied with mobile-money services, the service provider can provide information about how regularly MSMs receive money, pay bills, and make transfers to family members and business suppliers. Such information can develop a strong understanding and accurate scoring for MSM creditworthiness.

6.3.2 Wholesale Providers

Several retail businesses that have extensive supply chains that include small suppliers and merchants hold important information about the regularity of orders, inventory management, and payments to suppliers that can also be used for merchant underwiring, especially for many informal MSMs with no prior credit history.

6.3.3 Social Media Data

An alternate data source such as social media can be important to act as a proof of occupancy or stability of res-

idency. In cases where a merchant is advertising its product on social media, the data source may also become a way to gather feedback on the merchant and its products and, hence, to develop more accurate credit scoring.

6.3.4 Big Data

How big data is analyzed and eventually used for credit scoring is another area of innovation, as a number of mathematical algorithms are being developed for this purpose. For example, ZestFinance uses machine learning to gauge loan-repayment rates using 70,000 data points, including the speed of scrolling on a web page and reading terms and conditions.[44]

Possibly the most important aspects for merchant underwriting are simplifying the process and minimizing the required information. New merchant-acquiring models offered by service providers such as Square and PayPal are conscious of this important consideration expressed by merchants, and their business models enable quick time to market for new merchants, providing a major competitive advantage. To improve turnaround time for merchant onboarding and underwriting, many acquirer service providers are leveraging the use of technology and using risk-automation software. The key objective of utilizing underwriting software automation models is to enhance the merchant onboarding process without compromising risk-quality standards.

6.4 MERCHANT CREDIT RISKS

While considering a simplified and automated credit-scoring process, it should be looked into whether credit scoring for MSMs is needed at all. This is because the average value of transactions at such merchants is very limited, and the credit risks associated with chargebacks are also low. Consider a small barbershop or a street-corner merchant: Its average transaction value is relatively small. When all daily transactions are carried out face to face, possibly through QR-coded push payments, the chargeback risk of those transactions is considered to be low or zero. For MSMs accepting such transactions, the need to hold reserve funds for handling chargebacks is limited.

Unfortunately, in many emerging markets, the existing practices of delaying and, at times, not acquiring MSMs are based on applying heavy legacy underwriting standards that require documentation that MSMs may not be able to provide. Many small business owners may be disqualified immediately at the initial underwriting stage because they do not have access to or cannot provide a commercial business registration or bank account statement.

6.5 RECOMMENDATIONS

- Service providers should consider simplified criteria for evaluating the credit-risk score of MSMs and assess the need to evaluate the creditworthiness of MSMs upon access to EPA.
- Regulators should also have provisions to allow for the exemption or simplified creditworthiness-evaluation requirements for MSMs if they are applying for a basic level of EPA, have a limited-risk business, use a payment-acceptance instrument that carries limited risk, and are subject to a limited credit risk.
- Credit bureaus should consider developing new models for credit-risk scoring, including alternate data sources, to cover merchant communities that have been excluded from financial services.
- Service providers should adopt automated enrollment methods that categorize merchants with similar activities, business sizes, and geographical locations and specify proportional requirements with customized criteria and innovative models of credit-risk evaluation per category. Such an approach will provide an efficient method for mass enrollment of merchants while considering merchants' risks adequately.
- Service providers, merchants' facilitators, and payment gateways may need to develop their own innovative creditworthiness-evaluation models. Besides the dependence on credit-reporting companies, developing customized models of risk analysis for MSMs with little or no credit history would be a great advantage for such providers. Models that are based on public data, authorized access to customer information, supply-chain records, and social media could enable the adequate evaluation of credit risk while enabling access to finance to millions of MSMs.

Branch, a lender to small and medium-sized enterprises in Kenya, uses an alternate data–based credit-scoring model that analyzes SMS logs, social network data, call data, GPS data, and contact lists. Similarly, Tala, a lender working in Tanzania, determined that applicants who organized at least 40 percent of their contacts using both their first and last names were 16 times more likely to repay on time, because this tendency demonstrated the organizational skills of the borrower.[45]

PayPal

According to PayPal, the company holds 325 million active accounts and more than 20 million merchant accounts.[46] A key feature in the PayPal merchant value proposition is speed of setup, allowing customers with no previous registered accounts of their own to transact in just few clicks. PayPal solutions can easily integrate with various platforms through its own mPOS app (PayPal Here).

PayPal has a business model that makes it simple for merchants to set up an account as the primary merchant payment-processing platform. The set-up process requires no contracts, monthly fees, or sales account manager for personalized services. This service is more suitable for merchants with relatively low or seasonal business volumes per month, where accepting electronic payment is an added value. However, this may be a good option for merchants that cannot get merchant accounts of their own.

Merchants can apply to have a PayPal merchant account electronically. After completing the application process, merchants can receive payments in their bank account. A merchant account is what PayPal uses to route payments from customers' accounts to the merchant's bank account. Until the application is complete, PayPal may provide the merchant with a provisional merchant account. The merchant can accept up to $2,500 or 25 transactions from customers, and the merchant will not receive funds to its bank account until its account is fully approved. Approval takes one business day. After approval, there are no processing or disbursement limits.

The terms for account suspension are also quick and may seem abrupt to a merchant. Upon the first risk incident, the PayPal risk team may close the merchant's account with no prior notification or may subject the merchant to more stringent risk-mitigation terms to prevent future risk events. The cost-benefit analysis of employing this method may be useful for small merchants with monthly business turnover of less than $10,000.[47]

Ant Group Merchant Underwriting[48]

Before the emergence of automated consumer lending services in China, the credit market was very underdeveloped. More than two-thirds of the Chinese population did not have access to credit products or credit histories with the conventional financial systems. In 2015, the financial regulator in China began to allow private companies to enter the consumer credit-reporting business. Chinese tech companies soon rushed to the consumer credit market, using big data to assess credit and automated loan underwriting. This was possible given the abundance of user data and because algorithmic decision-making for existing internet services had already been established.

Companies such as Ant Group took advantage of supplementary data sources for their automated credit assessments. Given the wide adoption of such tech services as mobile payment and e-commerce in China, data points such as payment and money-transfer histories, online and offline purchases, and online credit card repayments were considered to have high predictive values for credit decision-making. For merchants with business licenses, the verification steps include the real-name verification of the merchant's AliPay account, a check of the legality of a merchant's business license, and a check on the authenticity of the merchant's commercial premises. Ant Group also evaluates the merchant's credit risk and provides different payment and credit services, such as merchant loans, based on the merchant's eligibility.

Automated underwriting has led to a rapid increase of available credit options. As a result, online consumer credit volume as a percentage of the overall consumer loan market in China increased from 0.5 percent in 2014 to 5.5 percent in 2016 and is expected to reach 9 percent in 2020, according to a report by the China International Capital Corporation.

7. Network Switches and Interoperability

TYPICAL MODELS

7.1 PAYMENT SCHEMES

The European Central Bank[49] defines a card payment scheme as *the set of functions, procedures, arrangements, rules, and devices* that enable a holder of a payment card to effect a payment and/or cash-withdrawal transaction with a third party other than the card issuer. The scheme is typically associated with a brand and provides rules for transaction routing, clearing, and settlement; obligations of issuers, acquirers, merchants, and cardholders; dispute-resolution and chargeback mechanisms; and domestic and cross-border rules upon using the brand. There are international and domestic payment schemes. For example, Mastercard, Visa, UnionPay, and Diners are all international payment schemes. Bancomat in Italy, Troy in Turkey, Rupay in India, Mir in the Russian Federation, and 123 in Egypt are all domestic payment schemes.

Payment cards may be issued by an issuer (a bank or service provider) or a merchant and may contain its brand along with the the brand of the scheme, making it a "co-branded" card. Each payment card may have one or more brands. For each transaction where the card is used, the rules that govern the transaction are the scheme rules associated with the brand selected between the acquirer, issuer, and switch. For example,[50] if a card is co-branded by Mastercard and Troy and used at a merchant POS in Istanbul, then the rules governing the transaction could be associated with either Mastercard or Troy based on one of the following conditions: (1) there is a preexisting agreement between the issuer (of the cardholder) and acquirer (providing merchant account) to select a certain brand upon accepting a payment, or (2) there is no agreement and, hence, the merchant or the acquirer bank can select which of the two brands' rules to apply.

International payment schemes not only set transaction rules but also bring payment innovations and solutions to local markets. While international schemes provide a more secure and interoperable environment, according to Capgemini, merchants typically pay 30–40 percent lower fees for accepting domestic debit cards compared to international debit cards, and smaller merchants pay 60–70 percent more than large merchants for accepting international debit cards.[51] Low transaction volumes and a higher risk of chargebacks are primary reasons why the acquirers charge smaller merchants a higher merchant discount rate. All financial institutions and PSPs connecting with the networks are required to meet and comply with the standards, rules, and requirements to enable transaction processing.

7.2 THE INTERBANK SWITCH

The interbank card switch is the routing center that transfers authorization requests, approvals, and transaction information to the appropriate receiver within a payment transaction. A domestic bank's payment switch is a system that can interface with domestic POS systems, ATMs, domestic mobile-payment systems, and internet-based commerce portals to route the transactions to one or more payment processors for authorization and settlement. The interbank switch is linked to the card brand used and is selected based on an agreement between the acquirer and the issuer service providers or a market- or international-level agreement. In some markets, the domestic service providers agree with the international schemes to route certain transactions through the domestic switch. So based on such agreements, a domestically issued Mastercard debit card used on an ATM or POS terminal could be routed among issuer and acquirer banks in a specific country using the country's domestic switch. Service providers take this approach mainly to use low-cost, no-frills, electronic-payment solutions for financial-inclusion purposes. The domestic switch could develop a domestic scheme that would potentially target electronic-payment services that focus on more inclusive finance. These include but are not limited to government pensions, social payments, and government employee payroll at a very low cost. However, the existence of international players could transfer experiences, technologies, and best practices and enhance the innovations.

By competing with international schemes, many domestic switches provide competitive fees for routing and clearing interbank card transactions on ATM and POS terminals. In many countries, domestic card switches route the transactions of cards having international scheme brands based on agreements between the two parties. For example, Egyptian Banks Company, the domestic switch in Egypt, signed separate agreements with Visa and Mastercard to route its domestically issued debit cards used on ATMs in Egypt. The switch can also be a catalyst to drive interoperability for mobile-money service providers by acting as the single point to route transaction traffic between mobile-money providers. It can be instrumental in the deployment of chip and PIN technologies with ready-made packages provided by switch vendors and can also support account-to-account and bill-payment enablement.

NEW MODELS

7.3 MOBILE-MONEY INTEROPERABILITY

Card platforms launched by card schemes (which were owned by bank consortiums) have been interoperable from the very beginning, and interoperability was the primary driver behind scalability. On the contrary, mobile-money providers began as closed-loop systems and started to become interoperable later. This historic difference explains some of the issues related to mobile-money interoperability.

Some mobile-money services are closed-loop systems and lack interoperability with other services. A closed-loop business model may protect the service provider's business revenues in the short term but eventually causes costly infrastructure duplications and dissatisfaction when customers are subjected to multiple different network experiences, rules, or costs even when operating in the same country. Another issue with the lack of interoperability is that customers or merchants may have to have more than one wallet to be able to pay and accept from everyone in the market, creating a burden on infrastructure and liquidity since precautionary balances need to be held in multiple accounts.

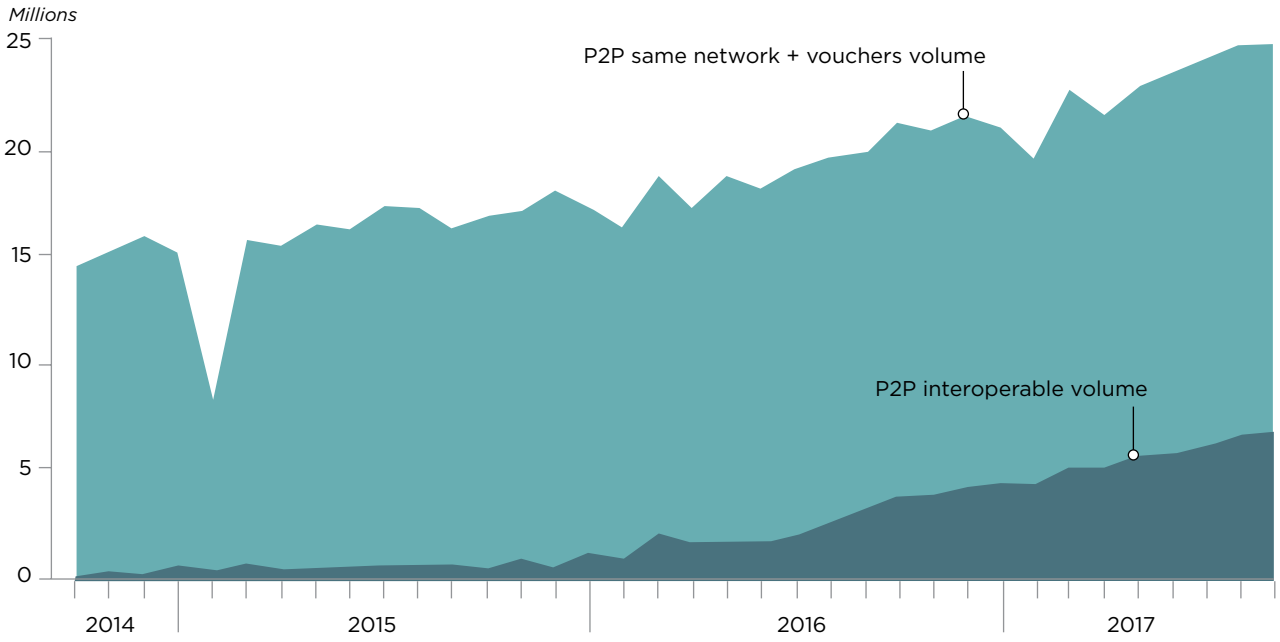
Interoperability provides customers with more choices, better transaction economics for all parties involved, and ease in conducting domestic cross-network transactions. As recommended by the European Central Bank, one of the primary oversight objectives for central banks should be to avoid market fragmentation when providing digital financial services. Hence, regulators should encourage interoperability among service providers, as it is consistent with the objective to improve the efficiency and effectiveness of the national payment system.

7.3.1 Scope of Interoperability

Interoperability is the ability of one customer of a mobile-money service provider to make a transfer to another customer at a second mobile-money service provider. Many types of transactions take place within mobile-money services, based on the owner of the account. There could be P2P, P2M, person-to-agent, and agent-to-person transfers on mobile-money accounts. Meanwhile, other types of connections enable transfers among e-money, card, and bank accounts, sometimes referred to as account-to-account transfers.

Mobile-money interoperability can be achieved through a central hub (switch), as in Egypt, Ghana, Kenya, and Madagascar; a fast payment system; or bilateral agreements among service providers, such as in Tanzania in 2015. (See the case study below.)

Figure 11: The Volume of P2P and Interoperable P2P Transactions



Source: *Building Inclusive Payment Ecosystems in Tanzania and Ghana* (CGAP).

In mobile payments, interoperability faces a number of challenges due to the absence of global rules and standards like those governing the large international card-payment networks. The absence of a global standard has led different markets to deploy different authentication techniques, pricing models, and transaction flows (credit push or credit pull), making mobile-money solutions inconsistent and fragmented across the globe. This inconsistency has sometimes made achieving interoperability of mobile-money acceptance for merchants a challenge.

However, for policy makers in emerging markets interested in expanding financial inclusion among the MSMs, mobile-money interoperability remains an important milestone in the development of MSM communities, providing them with better transaction-consolidation options, access to revenues, and pricing concessions. Further global efforts should work on developing interoperability among all channels, including domestic and international schemes. The deployment of QR codes, the use of merchant facilitators, and wider stakeholder collaboration at the domestic and global level may help resolve some of these challenges. Mobile-money operating models are changing. In some markets, the line is fading between P2P and P2M in terms of transaction usage, perhaps providing flexibility for future interoperability.

Connecting e-wallets to cards and bank accounts expands the utility and digital liquidity within the digital financial services ecosystem that was created mainly to serve the needs of the underserved or underbanked populations. One major obstacle for mobile-money networks has been the limited inflow of cash through agents and, hence, the limited circulation of money within mobile-money networks. The link between e-money accounts and bank accounts opens the inflow of funds to mobile-money networks and opens the market to several use cases that were previously impossible. Use cases related to mass transfers to mobile-money accounts, such as payment of salaries or pensions and linking merchants' mobile-money accounts to suppliers' bank accounts, will support the expansion of acceptance among MSMs.

Interoperability among mobile-money service providers can be expanded further to include agents' interoperability, where a customer can do a cash-in or cash-out transaction for his or her mobile-money account at an agent of a different mobile-money provider.

7.4 FAST PAYMENT SYSTEMS

Fast payment systems deliver funds to recipient accounts in real time or near real time 24 hours a day, seven days a week (24/7) and enable interoperability among e-money, cards, and bank accounts. Fast payment systems will be explained in detail in section 9.4.

In West Africa, eight countries are developing an interoperable system that will connect consumers with banks, microfinance organizations, and mobile-money service providers. The West African Economic Monetary Union is an example of this collaboration to drive interoperability and provide underserved customers with access to the financial system. The union will also enable many government-to-person and person-to-government payment solutions.[52]

Mowali (Mobile Payment Providers Interoperability)

Launched in 2018, Mowali is a joint venture for interoperability between mobile-payment providers Orange and MTN, bringing together more than 100 million mobile-money accounts and operations in 22 of Sub-Saharan Africa's 46 markets. Mowali also plans to enable interoperability between other digital financial service providers. The ultimate goal is to support all 338 million existing mobile-money accounts in Africa. Mowali enables sending money between mobile-money accounts issued by any mobile-money service provider in real time and at a low cost. This initiative enables wider collaborations, leverages infrastructures for use openly, saves costs of building new infrastructures, and promotes interoperability, providing the user with more choices. It would be essential for this interoperability platform to link to other service providers, including banks, other MNOs, and bill aggregators in countries of operation.

The New Payments Platform of Australia announced the release of new QR code standard specifications. The QR code standard will give payment providers the technical requirements needed to support real-time QR code–enabled payments. The New Payments Platform operates a fast payment system in Australia, providing access to different services via a series of APIs. The New Payments Platform's QR code standard is designed to "provide a single common code for payment solutions across multiple service operators, as well as the ability to facilitate payments among different payment schemes, e-wallets and financial institutions."

7.5 QR CODE INTEROPERABILITY

QR code interoperability enables merchants to accept different QR code–initiated payments issued by different service providers in a standard and consistent manner. It enables wider payment acceptance, delivering convenience, more choices, and incremental business volumes for merchants.

In 2016, EMVCo, the global technical body that manages the EMV specifications, established its QR Payment Mark to promote global interoperability across EMV QR code payments.[53] The EMV® QR Code Specification for Payment Systems[54] supports both merchant- and customer-presented QR code and static and dynamic QR codes. The standard has predefined places for international schemes (such as Visa, Mastercard, China Union Pay, and so on) as QR code providers and allows for domestic providers to include their own data in the same merchant QR code.

Hence, a common QR code may support multiple payment operators. Individual payment operators may define their own structures of merchant account information and make use of the common data fields, such as transaction, currency, and amount, contained in the common QR code. Currently, a number of countries, such as Hong Kong, have their own QR code standard, including their own providers.

While QR code has a huge potential to increase acceptance at MSMs, there might be security risks associated with its operation. If a QR code did not follow a standard security protocol, hackers might be able to access the mobile camera to record an image of a QR code, and the code may contain any type of data, not just payment data—it can also share links to phishing or malware sites. Some regulators applied limits to QR code transactions. For example, the People's Bank of China issued regulations limiting any QR code transaction to $80. Such limits are not applicable in most countries.

7.6 RECOMMENDATIONS

- Merchants in general should be enabled to accept electronic payment from all payment instruments provided by all service providers. Therefore, the development of platforms that enable merchants to accept multiple mobile-money providers, cards, and even bank transfers should be encouraged by proper standards and by interoperability infrastructure.

In 2019, Bank Indonesia announced the launch of the Quick Response Indonesia Standard (QRIS). The standard enables universal digital transactions within Indonesia. "QRIS allows QR-code-facilitated payments to be interconnected and interoperable through a single standardized code," according to the bank. The QRIS standard is based on the EMV international standard.

- Regulators should ensure that the payment market is not fragmented and that the interoperability of payment systems and services is set clearly as an objective of overseers of the national payment system.
- There may be different levels of interoperability among mobile-money service providers based on the level of market maturity. The regulators and interoperability system operators need to consider the market conditions while developing the rules for interoperability. In many markets, most of the mobile-money providers will welcome interoperability with cards and bank accounts, while different financial aspects could drive the willingness to achieve interoperability in P2P payments, P2M transfers, agents' cash-in and cash-out, bill payment, and government payments and collections.
- Establishment of the retail interoperability infrastructure may not be enough to ensure healthy market progress. The market authorities need to have a continuous dialogue with service providers to ensure their buy-in and to facilitate the use of the infrastructure. The interoperability infrastructure will not be fully utilized without marketing campaigns and developing integrated use cases at the service provider product profile. Service providers will need to train merchants and possibly add branding to accept payments from other providers.
- It is crucial for market stakeholders to hold dialogues to enhance market practices, agree on standards, or develop protocols and interfaces for integration of services. The regulators should encourage such dialogues and establish them if the market did not take the initiative.
- There is *no* global standard for mobile-money transactions. Some service providers in certain countries have agreed upon interoperability protocols. However, the lack of standards makes it difficult to enforce interoperability due to differences in data and messaging formats, exchange channels, and the transaction workflow. Some initiatives have recently started to overcome these challenges. EMVCo's standard for QR code possibly can be considered as a successful example.
- It is not preferable for financial regulators to enforce fees or pricing policies, including for interoperated transactions. However, the regulators should understand clearly the economics for payment service pricing, including dynamics, drivers, and externalities. Regulators should ensure that market prices are fair

Tanzania is a market in which mobile service providers agreed voluntarily to establish an interoperable service. Three major players in the mobile-money segment—Airtel Money, Tigo Pesa, and Vodacom M-Pesa—enable P2P interoperability between accounts. When interoperability was introduced, Tigo Pesa tripled its P2P transfer value between 2015 and 2016, and the other providers displayed similar growth. Tanzania is the first market where mobile-money providers paid interest on wallet floats, bringing new loyalty dimensions to mobile-money consumers and merchants that accepted mobile payments.[55]

Tanzania generates 95 million mobile-money transactions per month. The cost-benefit analysis for such a model is great for the country, enabling a fast-tracked financial-inclusion effort coordinated and aligned between regulators, mobile-money service providers, consumers, agents, and merchants.

The process of launching and running interoperability in Tanzania has been influenced by the following factors:

- Regulatory environment: Government and policy makers kept in close contact to align timing, benefits, costs, and risk of interoperability.
- Timing of launch: Resources and investments are required for the implementation of interoperability. Therefore, timing must be carefully considered.
- Trust: Interoperable mobile-money solutions require trust between partners, as they have to expose their systems through integration. Reliable systems and a solid operational foundation ensure the trust necessary to merge systems successfully.
- Risk mitigation: As additional complexity is added through interoperability, recognizing risks and acting upon them are vital.

and sustainable for consumers, merchants, and service providers. Regulators may need to lead a dialogue among stakeholders, including representatives of merchants, to adjust pricing, aiming at expanding payment services and protecting consumers. However, the consumer protection authorities or other authorities concerned with financial consumer protection might recommend caps on service fees if they are not convinced that these are fair to a large segment of consumers.

- The integration between mobile accounts on one side and cards and bank accounts on the other is very useful in bringing cash to the mobile-money environment. Most mobile-money providers will favor connecting to cards and bank accounts; in some cases, this can be a starting point for a larger scope of interoperability. However, markets need to push for full interoperability among different types of financial service providers.

8. Authorization and Authentication

Authentication is the process of ensuring that the payment transaction has been initiated by an authorized user. Authorization is the approval by the payer's financial institution that the payer has sufficient funds to pay for the transaction and, sometimes, the approval by the merchant's financial institution that the transaction is within the limits of the merchant.

8.1 AUTHENTICATION

In a card-based electronic-payment transaction flow, authentication and authorization are two key aspects of the transaction communication process. Authentication is the process of confirming an account holder's credentials with the issuing entity. It refers to the first half of the transaction communication process, in which the merchant-acquiring bank transmits transaction details to the issuer through the payment network for authentication. The authentication process is engaged mostly with the payer, but it helps prevent chargebacks and protects the merchant from any funding issues.

In a simple authentication process, the issuer checks various account details such as card number, card type, card security code, and cardholder billing address to ensure accuracy. Issuers also have various procedures in place to ensure that a transaction is not fraudulent to protect the security of the account holder. Once authenticated, the merchant-acquiring bank receives the communication from the network processor and authorizes the transaction for payment acceptance and deposit to the merchant's account.

8.1.1 Strong Authentication

Due to increased fraud and security concerns, and reflecting decreases in complexity and cost of implementation, the use of **strong authentication** methods is now becoming common for e-commerce and m-commerce transaction authorizations. One commonly used method is multifactor authentication for customer verification, which requires at least two different factors of proof (also referred to as two-factor authentication). The following three types of authentication factors are recognized:

- **Type 1: Something you know.** This authentication factor includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.
- **Type 2: Something you have.** This type includes all physical items, such as keys, smartphones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.)

PayPal provides an example of multifactor authentication supporting e-commerce since it currently offers at least two different multifactor options. One option involves a credit card–sized device that produces on demand a one-time-use six-digit PIN. The second option sends an SMS text message with a six-digit PIN to the user's cell phone. In either case, the PIN is used alongside the name and password credentials to gain access to the PayPal account.[56]

- **Type 3: Something you are.** Type 3 includes any part of the human body that can be offered for verification, such as fingerprints, palms, faces, retinas, irises, and voice.

By combining two or three factors from the above categories, a multifactor authentication can be integrated for e-commerce or m-commerce purposes. Such standards are preferred over simple authentication techniques, as they are harder to compromise. For simple authentication, only a single password is required, and an intruder has to have only a single attack skill and wage a single successful attack to impersonate the victim. With multifactor authentication, the attack must have multiple attack skills and wage multiple successful attacks simultaneously to impersonate the victim. This is extremely difficult and, thus, a more resilient authentication solution.

8.1.2 3D Secure

In the payment industry, a number of innovative ways to secure CNP transactions or e-commerce are evolving. The general rule for these methods is to confirm to the card issuer that the transaction is carried out by the actual cardholder. This is done by reaching out to the cardholder through a different channel or by asking for information that is known only to the cardholder (mostly dynamic). Examples include 3D Secure, also known as Payer Authentication, which is a security protocol to prevent fraud related to CNP e-commerce transactions using credit and debit cards.

3D Secure is essentially a messaging protocol that promotes frictionless consumer authentication and enables consumers to authenticate themselves with their card issuer when making CNP purchases. The additional security layer helps prevent unauthorized CNP transactions and helps protect the merchant from exposure to CNP fraud. The service is provided by Visa as Verified by Visa or Visa Secure.[57] A similar service called Mastercard Secure Code is provided by Mastercard.[58]

The initial version was launched in 2001, but in 2018, EMVCo overhauled the standards and released an updated version 2 for 3-D Secure. Under the current specifications, the three domains consist of the merchant/acquirer domain, the issuer domain, and the interoperability domain (for example, payment systems). EMVCo maintains the specifications and the test platforms to facilitate the functional testing of 3D Secure solutions.[59]

8.2 AUTHORIZATION

Once the transaction is authenticated, the issuing bank will check that the cardholder has enough funds or credit to pay for the transaction. The issuing bank will place an authorization hold in the amount of the purchase on the cardholder's account. The authorization process also allows the merchant bank to initiate a payment deposit in the merchant's account. The merchant's POS terminal will collect all approved authorizations to be processed in a "batch" at the end of the business day. Every retailer has a purchase limit above which they must seek authorization before they can complete the sale. Authorization is used to control card fraud.

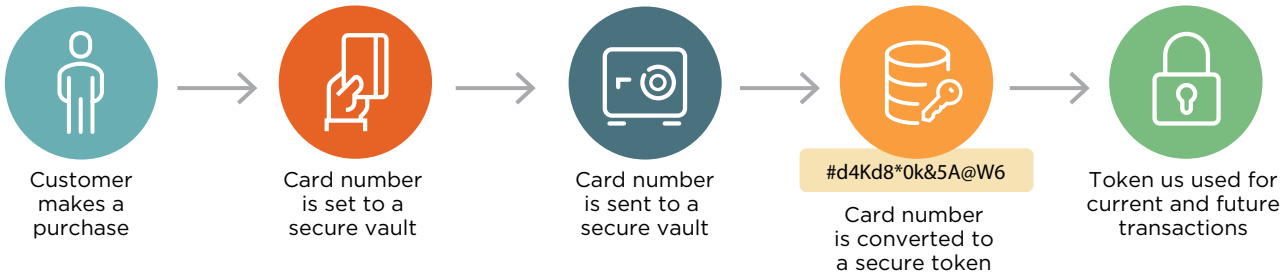
If the authorization is declined, the POS terminal will return a response code explaining why. Some of the key response codes include incorrect credit card number or expiration date (meaning the authentication failed) or insufficient funds. Some issuers reject international charges. Authorization may also be declined if the issuing bank or the payment process experiences technical issues while the transaction is being processed. In addition, if fraud is detected using detection tools, some banks will reject the charges as a fraud-prevention measure.

The new authentication and authorization technologies try to strengthen the methods used to authenticate the customer by means of one-time passwords, reaching the customer via alternate channels, such as mobile phones, and hiding the card or transaction account information through tokenization, virtual card numbers (VCNs), or addressing services.

8.3 TOKENIZATION

Tokenization is widely used in large schemes and is expanding as a practice to protect customers' sensitive payment details. Tokenization enables the replacement of payment details with a stand-in token, ensuring the safe storage of payment details in e-wallets and at merchant e-commerce locations where payments recur. A payment token is a substitute value of the card payment account number (PAN) that passes typical validation rules of the PAN but is generated within an identified token bank identification number range that cannot be conflicted with a

Figure 12: Card Tokenization



Source: https://www.centurybizsolutions.net/business-tips/4-benefits-of-using-a-tokenized-credit-card/

real PAN range. The use of tokenization is more secure than encryption because, unlike data that is encrypted, tokens are not mathematically reversible with a decryption key and the PAN is never displayed. Tokenization is expanding as a cost-effective solution, enabling stronger security measures for payment services. Tokenization is replacing card and payment details in recurring billing and in e-commerce.

The use of payment tokens is controlled by token domain-restriction controls that may include dynamic token cryptograms, POS entry mode, and other parameters managed by the token service provider. Such controls protect the payment tokens from unauthorized or fraudulent use commonly associated with typical PANs.[60] The tokenization of payment data has become an innovative way to replace sensitive data—typically, payment card or bank account numbers—with a randomized number in the same format but with no intrinsic value of its own. This practice was adopted to reduce high levels of fraud associated with stolen payment card information from magnetic stripe cards and then cloned for e-commerce and m-commerce fraud. Similar to how EMV chip cards were designed to fight fraud for card-present transactions, tokenization was designed to fight online or digital breaches.

Token service providers are authorized service providers that provide payment tokens to registered token requestors. By end of 2019, EMVCo had registered 35 token service providers.[61] Tokenization protects online shopping activities by replacing customers' payment details with a token gateway. Token gateways provide a single software interface to multiple token service providers and ensure that merchants are constantly aligned with the latest card scheme tokenization specifications. Tokenization delivers advanced security and cost savings by reducing instances of fraud and liability. Merchants can significantly reduce overhead by implementing a card-on-file[62] tokenization system.[63]

Apple Pay tokenization: The payment schemes facilitate an identification and verification process with the card issuer (the card image may be loaded, or the information may be entered manually); once the consumer passes that process, the payment schemes generate a token mapped to the card and send that token back to the wallet provider. The token is then passed during the transaction.

Android Pay tokenization: When the card information is loaded into the app, Google creates a stand-in token to represent the actual account number. When a customer transacts at a merchant, Android Pay doesn't send the customer's actual credit or debit card number with his or her payment details. Instead, Android Pay uses a virtual account number to represent the account information, so the card details remain safe. This provides added value and security to the merchant through better fraud controls and a lack of concern about the safe storage of cardholder account details.

Tokenization within apps: If consumers buy something straight from an app on their phone, and if their phone contains a token, none of these retail apps have access to their credit card details. Using a tokenized account can also make it easier to check out, as many apps will link directly to their stored shipping information.

8.4 SECURE REMOTE COMMERCE

e-Commerce has been around since the early 1990s, and even though the processes have evolved, the e-commerce environment in general has had many different integration models coupled with a variety of implementation practices, all lacking a set of common or standardized specifications for this environment, resulting in fragmentation, complexity, and inconsistency. While the overall security of payments in the physical POS terminals improved due to the adoption of global EMV specifications, a lack of common industry specifications for a number of potential remote commerce payment scenarios created opportunities for attackers and hindered the progress made against payment-related fraud.

To address this issue, Mastercard and Visa in 2018 launched a standardized method for e-commerce checkout based on a unified, streamlined checkout framework proposed by EMVCo in November 2017. This method is known as Secure Remote Commerce, providing a unified digital checkout specification. This is an evolution of remote commerce for secure and interoperable card acceptance established through a standard technical framework and specification. It provides a merchant with a secure way to request and receive interoperable payment data used to process accepted cards in a remote commerce transaction. Since Secure Remote Commerce is platform agnostic, the technology allows consumers to choose the payment method they wish to use.

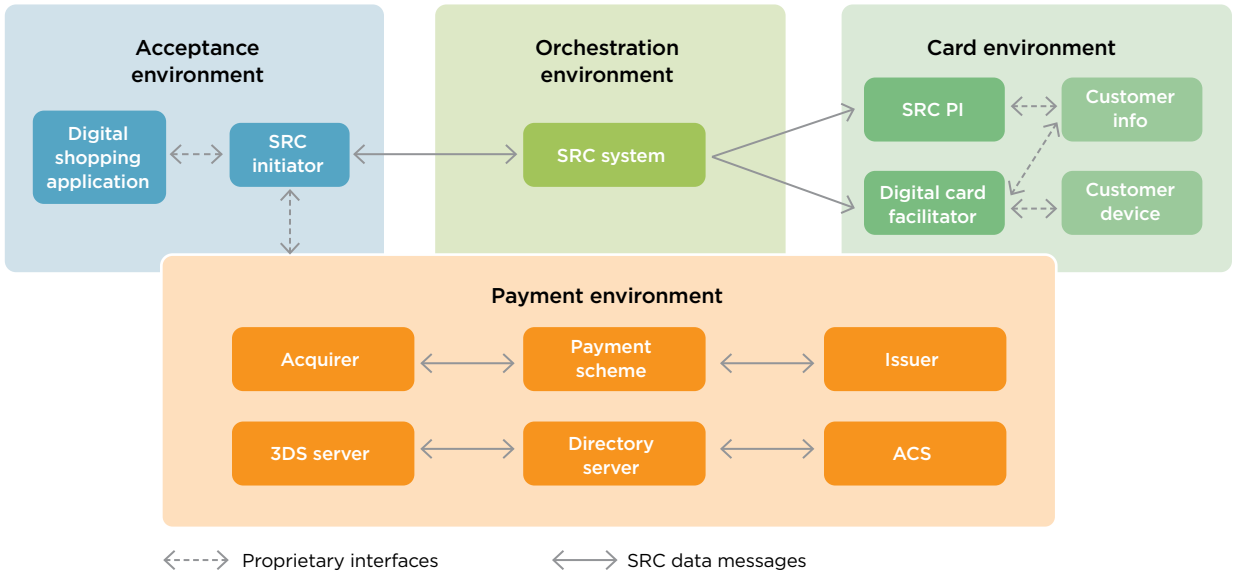
According to the framework, Secure Remote Commerce will provide simplified and efficient integration and interfaces between payment ecosystem stakeholders, facilitate interoperable and secure payments, and decrease the vulnerability of shopping websites and mobile shopping applications via the secure transmission of payment data and related checkout data. This is in addition to other features, such as reducing the abandonment of shopping carts by decreasing the number of repetitive manual PAN entries and providing integration options for EMV specifications, such as payment tokenization and 3D Secure authentication (version 2.0).

Tokenization has a major role to play in simplifying the e-commerce checkout process. A token-only world is within reach, and Secure Remote Commerce will support this by building on the EMVCo tokenization standards. It renders the credentials useless to fraudsters and reduces the risk for merchants. It also provides consumers visibility into where their credentials are stored and how their data is used. Potential use cases include payments initiated using a device that accesses digital card credentials stored outside merchant environments, during a guest experience at a merchant, or during a merchant card-on-field experience.

8.5 VIRTUAL CARD NUMBER

VCNs are digital one-time-use versions of existing customer PANs. VCNs are uniquely generated for each customer transaction but billed back to the same customer payment account. A VCN is a 16-digit card number (PAN) with an expiry date and a security code.[65] A VCN can provide a simple and secure payment mechanism in situations ranging from business-to-business supplier pay-

FIGURE 13: A High-Level Overview of Secure Remote Commerce Participants Based on the EMVCo Specification[64]



ments to e-gifting and e-commerce. VCNs may display different brands like international card schemes, among others, and may be issued for use with credit, debit, prepaid, and commercial payment products and solutions.

Depending on the issuing financial institution or network, VCNs may include such features as load options or spend controls for use with specific merchants at specific time periods and for specific types of purchases. Some VCNs can be used with e-wallets. VCNs offer an added layer of security to protect account data; enhance control; increase flexibility, speed, and foreign-exchange transparency; reduce costs; and simplify reconciliation processes.

8.6 ADDRESSING SERVICES

Traditionally, a payer will need to know the payee's bank account information to make a payment. Account information would include the payee's bank name, bank and branch code, and account number, or the card number. Such information could be forgotten or easily keyed incorrectly. With the trend of masking the account and card information to avoid fraud, using an alias or an alternate address has become the preferred solution for many payment systems, especially fast payment systems. Using an addressing service means mapping a user's full account information to an alias name or address that can be remembered and shared easily, such as a mobile phone number, an email address, or even a nickname. The alias should be unique, and all mapping between addresses and account information should be registered and stored at a service provider. The addressing service provider would receive a nickname or email address from a participating PSP, seek the associated account information, and reply back with the account information. Hence, the transaction information exchanged among end users would include only aliases and addresses, while the PSPs would exchange real account details.

8.7 RECOMMENDATIONS

- Strong authentication is important to secure consumers' funds, but there should always be proportionality between risks and requirements. Hence, regulators should consider easing the security requirements for basic accounts or less risky transactions, such as card-present, credit-push, and small-value transactions. Strong authentication may require more expensive systems, sophisticated tools on the client and provider levels, and expensive maintenance. It is crucial for regulators to mandate proportional requirements where requirements are proportional to the risks. In low-fraud payment instruments or use cases, it would be important not to request high security measures.
- Service providers should seek to secure card and account numbers through such methods as aliases or addresses, tokenization, VCNs, and others, and regulators should encourage the adoption of security for the payment ecosystem. Such an approach will reduce the possibilities for fraud and, hence, reduce the overall cost of managing payment transactions.
- For countries that are developing national digital ID systems, it would be crucial to develop a financial-authentication module that is linked to the system. The financial-authentication module allows the separation of the authentication process from the financial service. Hence, any financial institution would be able to provide its services to any customer based on an independent third-party authentication process that simply verifies the identity of the person receiving the service, either through a private key, biometric measurements, or both.

The Australian **New Payments Platform** includes an addressing service named PayID that allows customers the option of registering their phone number, email address, or Australian business number and a "display name" in a secure central repository via their financial institution. The PayID is then linked to their bank account details and used to direct a payment into a linked account—it cannot be used to withdraw from that account. A PayID name is recorded with the proxy (email address, phone number, or Australian business number) and account details. Message flows and rules for the New Payments Platform have been designed to enable PayID name validation for all PayID-initiated New Payments Platform payments. This particular feature will enable payers to check and confirm a payee before authorizing a payment, reducing the incidence of misdirected and mistaken payments, including payments to fraudsters and scammers purporting to be a genuine payee.[66]

9. Clearing and Settlement

TYPICAL MODELS

9.1 CLEARING PROCESS

In card acceptance, the merchant transmits all transactions to the acquirer bank as a batch at the end of the day. The acquirer bank processes batches received from merchants and sends the batches to the card network, where each sale is routed to the appropriate issuing bank. The previous process is called the cards transaction clearing.

The clearing messages include only data and do not exchange or transfer funds, processes that occur later, during the settlement process. The acquiring bank must comply with the payment network's clearing timelines for transaction processing. Every day, millions of transactions are cleared globally through VisaNet, Mastercard's GCMC, China UnionPay, Discover, and tens of domestic networks. The networks send cleared transactions data to the issuers and assess issuer's and acquiring fees.

There are two different types of payment-processing systems. The first is a dual-message system for use with credit cards and debit cards that authenticate through cardholder signatures. The second is a single-message system for use with ATMs and POS terminals that authenticates debit transactions through cardholder PINs. However, the clearing and settlement time frame is typically shorter in the single-message system than in the dual-message system.

When the acquirer bank is the issuer bank, there is no interbank clearing process, and the accounts of the customer and the merchant are debited and credit directly at the bank. The clearing processes for many mobile-payment solutions facilitating P2P and P2M transactions are different and might happen more than one time per day, speeding the merchant's access to funds, a critical consideration for MSMs.

9.1.1 The Shift from Two-Stage to Single-Stage Clearing

The shift from a two-stage to a single-stage clearing process in card payments illustrates the shift to a simpler clearing process in which clearing is completed once the transaction payment is initiated. Single-stage clearing reduces the cost of processing, enables faster payment, and sidesteps the traditional infrastructure for authorizations, clearing, and settlements. This is also suitable for small-value and frequent transactions, which are common for P2P and P2M transactions involving MSMs. A number of domestic switches apply single-stage clearing for the reasons mentioned earlier.

NEW MODELS

9.1.2 The Shift from Credit-Pull to Credit-Push Models

The traditional payment to merchant through cards applies a credit-pull model, where the transaction starts from the merchant POS terminal and pulls the funds from the card-holder account. In mobile P2P and P2M payments, the transaction starts from the mobile phone of the payer, and the credit is pushed to the merchant's account. Hence, it is a credit-push model. The difference between both models is far beyond the flow of the transaction and who starts it; this section explores further differences.

In the mobile P2P model, the recipient receives its payment on a real-time or near real-time basis, while in the traditional model, it takes a number of days to complete the clearing and settlement process. Mobile P2M solutions are particularly interesting to MSMs, as they offer faster access to funds and cost less. P2M models bring a number of key considerations. Once a user executes a compliant transaction, it cannot be revoked. Funds are transferred to the merchant's account fast. The sender may have no recourse in the event of a transaction dispute, but the service providers are striving to improve customer support, and many agree to investigate disputes if the program guidelines were correctly followed. If P2P solutions are used with linked traditional payment card accounts, such as for payment to merchants through e-wallets linked to a card, the standard network liability-shift rules will apply. So in the case of a mistake or error, the liability will be on the payer, not on the merchant as a payee.

The shift toward push payments has enabled better security in payments, including reduced sharing of confidential payment details, and limited fraud risk associated with merchants' storing of card details. In a push-payment transaction, the user is empowered to initiate the processing of the payment transaction, taking full responsibility for the payment decisions. Because the user controls the transaction handling, reasons for chargebacks are limited unless processing errors occur, the payment instrument is stolen and PINs are released, or there are other concerns related to undelivered goods or services, especially in cases of non-face-to-face transactions. For these exceptions, the user should be able to refer back with relevant details to the service provider. Anyhow, the possible cases for fraud and chargebacks are limited compared to a credit-pull model. Service providers should address the possible cases of dispute through adequate dispute procedures and mechanisms.

Due to reduced fraud concerns, push payments reduce merchant's credit risk, as push payments are initiated by the user. Because settlement of the merchant account is completed instantly and is irrevocable, acquiring banks and merchant facilitators should consider that mobile-money merchants bring minimal or no credit risk. However, concerns related to chargebacks could still exist in limited cases related to non-face-to-face transactions and a few other cases. In general, the merchant credit-evaluation process should be rationalized for credit-push transactions, if it is still required at all.

Deploying push payments for merchants through QR code or direct P2M transfer is simple, fast, and cost effective. In many cases, it reduces the merchant service fees paid to the merchant acquirer compared to what is paid in the credit-pull model mainly because of low fraud levels and the absence of corresponding credit risks posed for MSMs. In addition, it eliminates the high costs associated with POS devices, including their maintenance costs. It is worth noting that international card schemes apply credit push at some products. For example, Visa Direct has use cases that implement push payments, such as payroll, government-to-person disbursements, and remittances.

PayTM in India launched a mobile-money payment application specifically for merchants' acceptance. PayTM added a new feature to its latest app to help small and medium-sized merchants accept payment cards. The merchant discount rate is zero for UPI, RuPay, and PayTM debit transactions.[67]

9.2 SETTLEMENT

TYPICAL MODELS

9.2.1 Settlement Cycle for Card Network Payments

Upon completion of the clearing stage, and as part of settlement, by transaction date plus one or two days (T+1 or T+2), the issuing bank transfers the funds, less the interchange fee, which it shares with the payment network. The payment network pays the acquiring bank its percentage due from the remaining funds. The acquiring bank credits the merchant's account less a merchant service fee. The issuing bank posts the transaction information to the cardholder's account. The issuing bank either debits the account immediately, in case a debit card was used, or, if a credit card was used, waits for the cardholder to receive the statement and pay the bill later.

NEW MODELS

9.2.2 Immediate Crediting of Merchant's Account

Crediting merchant accounts in real time is becoming popular with many new push-payment solutions. In a typical P2P or P2M transaction, the recipient is credited immediately, although the settlement between financial institutions of the payer and payee may happen later. Enabling real-time retail payment infrastructure is a key motivator to expanding EPA and electronic payments in general.

Real-time payments are not just about the speed of payment; when combined with other aspects, such as low cost, improved service delivery, a trusted service provider, and so on, they can enhance the value proposition for the solution. For example, combining QR codes with instant payments has created new dynamics and a new value proposition. APIs combined with instant-payment mechanisms have also created a compelling new value story for merchants, enabling customers to shop and pay on the spot, with no merchant fees and enhanced speed to access funds.

The evolution of QR codes has also allowed them to become the preferred payment-acceptance method in some of the world's largest mobile-payment markets, such as Asia. In China, both Alipay and WeChat have integrated instant-payment capabilities besides using QR code vouchers to add loyalty elements to their e-wallet offerings.[68] As the use of instant payments expands, they may lead to a transformation in the digital-payment landscape, completing an end-to-end instant-payment journey that includes reconciliations and fraud monitoring.

Mastercard and Unilever have teamed up in Kenya to deliver an initiative for MSMs called Jaza Duka ("fill up your store"). The goal of the program is to help small businesses build the required credit history to be able to access credit in nontraditional ways. Small businesses dealing in cash do not have the right document trail to prove their creditworthiness. Jaza Duka enables the purchase and payment history of a business to be used to build a credit history. Unilever tracked small merchants' purchases from suppliers. If the merchants have consistent orders with one supplier for $50, they can qualify for an interest-free line of credit for $120 to purchase supplies. The program also delivered training for local capacity building from TechnoServe.[69]

9.3 SUPPLY-CHAIN CREDIT AND CASH-FLOW CYCLE

Despite the enhanced speed of payments in various mobile-money solutions, many MSMs view electronic payment as an inhibitor to their business model because they lack instant access to cash to pay their suppliers. This view sheds light on the importance of expediting and localizing electronic-payment solutions within the merchant supply chain to meet the need for immediate access to funds. Digitizing the merchant supply chain and providing fast access to funds is important but insufficient. MSMs lack access to credit to enhance their working capital and rely on the proceeds of daily sales to stock their business supplies. Such MSMs may also lack access to insurance and other financial products to protect and grow their businesses.

This process is important to suppliers because it enables an electronic-payment method for collecting the proceeds of sales, facilitates the collection of funds, reduces the risk of transferring cash, and automates the calculations of merchants' balances with the supplier. Global corporations that supply goods to retail markets have strong reasons to digitize the supply chain and to collect sales by electronic payment. The suppliers' acceptance of electronic payment will motivate their merchants also to accept electronic payment, thereby completing the full sale-and-payment cycle and replacing the existing closed loop of cash with a closed loop of electronic payment. Digitizing the merchant supply chain with faster payments will enable wider payment acceptance and localized capacity building and will help create new merchant-acceptance habits.

9.4 FAST PAYMENT SYSTEMS[70]

In addition to innovations in existing retail payment systems, fast payment systems (FPS) are emerging as a new type of payment system driven by changes in economics, demographics, and customer needs for faster, cheaper, and more accurate means of making payments. According to the Committee on Payments and Market Infrastructures, a fast payment is defined as a payment in which the transmission of the payment message and the availability of "final" funds to the payee occur in real time or near real time and as near to 24/7 as possible.[71] Currently over 60 countries across the globe have an FPS in place, and several others have announced their plans to go live before 2023. The basic principle among all the countries remains the same—that is, to provide a real-time, 24/7, fund-transfer facility. In addition, a few countries have payment systems that resemble FPS, such as interoper-

able mobile-money systems, but are not classified as fast payments according to the Committee on Payments and Market Infrastructures' definition.

FPS as a mode of payment attempts to provide an additional channel to address the low adoption of electronic payments among consumers and small businesses. It has enabled the completion of time-sensitive payments quickly and with finality, thereby increasing end-user confidence in digital payment methods. The following characteristics can be associated with FPS:[72]

- Instant settlement finality for both the payee and the payer, and the availability of final funds to the payee or beneficiary occurs in real time. In other payment modes, while the payer's account is debited in real time, the funds may or may not be made available to the beneficiary immediately. (This depends on the agreement between the acquirer and merchant.)
- Transactions can be made through new modes of interfaces, such as mobile applications from third-party providers.
- New access channels and transaction-initiation methods, such as QR codes, have been introduced.
- Membership to FPS is broader, and non-banks can also participate as both direct and indirect participants.
- Channels innovation and newer payment-transaction flows are introduced through use cases such as request to pay, welfare payments, and salary payments.
- Payments made with the help of such aliases as phone numbers, email address, and so on are increasing user convenience.

Immediate settlement of payment also tends to give FPS a near-cash-type characteristic, thereby increasing consumer confidence in it as a mode of payment for small retail payments. To facilitate a near-cash, seamless experience for all types of users, focus has been increased on the interoperability of payment systems and types. Technical innovations have helped support interoperability. In many countries, third-party service providers have used the FPS infrastructure to design and provide innovative payment solutions to the end customers. It has provided the basis for service enhancements and value-added services.

FPS adoption, however, must be balanced with appropriate safeguards and risk-management frameworks. It is important to ensure that innovations in the payment space do not come at the cost of overall security and safety. It is crucial, for example, to put in place a robust fraud-mitigation system to ensure the health of the system. Clear dispute-resolution mechanisms are needed to address concerns, such as when a payment is accidentally made to the wrong recipient. In addition, the risk of social-engineering attacks, such as phishing, can be higher with fast payments than with other modes. This concern needs to be mitigated with an appropriate monitoring system, fraud-prevention tools, and end-user training.

9.4.1. Growth Drivers for FPS

Adoption and uptake of FPS services vary significantly between countries based on the following characteristics:

a) Coverage and openness of the system: The following may ensure wider coverage and openness of FPS:
   - Support for both push and pull payments: Accommodation of both types of payments helps in offering a wider range of use cases and services to the end customers.
   - Participation of non-banks and technology companies: The presence of more participants makes the system more valuable to each participant. The more-traditional participants of the FPS ecosystem are banks; however, inclusion of non-banks and technology companies, such as mobile network operators and mobile-money operators, will provide FPS with a wider user base and help boost adoption.
   - Financial inclusion as a motivation to introduce FPS: Countries may witness widespread adoption owing to affordable pricing and efforts from the regulator or government to boost adoption.

b) Access channels and ease of use: FPS is a new technology that various stakeholders may be unfamiliar with. Limitations in access to the system or a complex user experience could make it inconvenient to use the services, which in turn pose a significant challenge to adoption and usage. The following may ensure easy accessibility and a more user-friendly experience:
   - Accessibility via everyday-use devices: Many FPS have demonstrated the importance of accessibility to services through devices such as mobile phones and computers as a driver for adoption.
   - Use of aliases (mobile numbers, national IDs, virtual payment addresses) makes it convenient for users to avail the services offered through FPS without revealing their actual identity, which in turn promotes uptake.
   - FPS accessibility via an API and the usage of international standards, such as ISO 20022, facilitate payment service providers to connect to the system and structure their offering.

c) Technology and preexisting market context: Uptake is likely to be higher in countries where the preexisting

market context enables use of real-time payments. The following technological and market factors play a role in the adoption of FPS in a country:

- Level of penetration of smartphones and internet services
- Quality and payment speed of other payment options (checks and so forth)
- Level of market competitiveness in the payment space

9.4.2. Motivations to launch FPS:

Over 60 countries have live FPS, and the motivation to implement FPS has varied because of the following factors (followed by detailed examples from Australia, Europe, India, and the United States):

- Countries were motivated to introduce FPS primarily to introduce real-time payments. The introduction and adoption of FPS has been either market driven, regulator driven, or a combination of the two.
- The desires to enhance customer experience and drive innovation have been key for regulators, operators, and participants. Pursuing financial-inclusion objectives has also served as a driver in select economies. Convenience and safety are two key factors taken into consideration while introducing FPS.
- Regulators' initiatives and government push are believed to be the drivers for FPS adoption as well. In some countries, the government was also involved during FPS conceptualization.
- While some countries initially witnessed resistance from participants owing to comfort with existing systems, collaborative efforts from the central bank helped drive adoption by participants.

The Unified Payment Interface (UPI) was launched in India in 2016 as a fast retail payment system. It is an account-to-account transfer process in real/near real time on a 24/7 basis, albeit with caps on value, using simplified details/pseudo addresses instead of account names, account numbers, and bank/branch codes. Its success was propelled through the following enabling, forward-looking policy initiatives with a long-term view to transforming access to the payment system and financial inclusion:

- The launch of Aadhaar to establish digital identities for more than one billion people
- The Jan Dan Yojana Initiative, which created bank accounts that connect with Aadhaar digital identities
- Connecting people through mobile phones and post office accounts to grant access to their bank accounts

The National Payments Corporation of India developed UPI as a common interface or platform for retail digital payment systems in India, known as the JAM Trinity (Jan Dhan, Aadhaar, and Mobile), providing the end user with more and better choices for accessing the financial system. UPI enables architecture and a set of standard API specifications to facilitate digital payments using a mobile phone.

Mobile phone penetration in India is high, and adoption of smartphones, data, and the internet is growing. UPI allows users to send or request money instantly from their bank accounts using a mobile phone as the primary device for the transaction. Anyone with a bank account can create a virtual payment address (VPA or UPI ID) and start transacting using a mobile phone. The virtual payment address becomes a person's unique payment identity and abstracts the need to share bank details while transacting. UPI considerably simplifies digital payment by combining mobile payments with a unique payment ID to make it a low-cost payment-acceptance device.

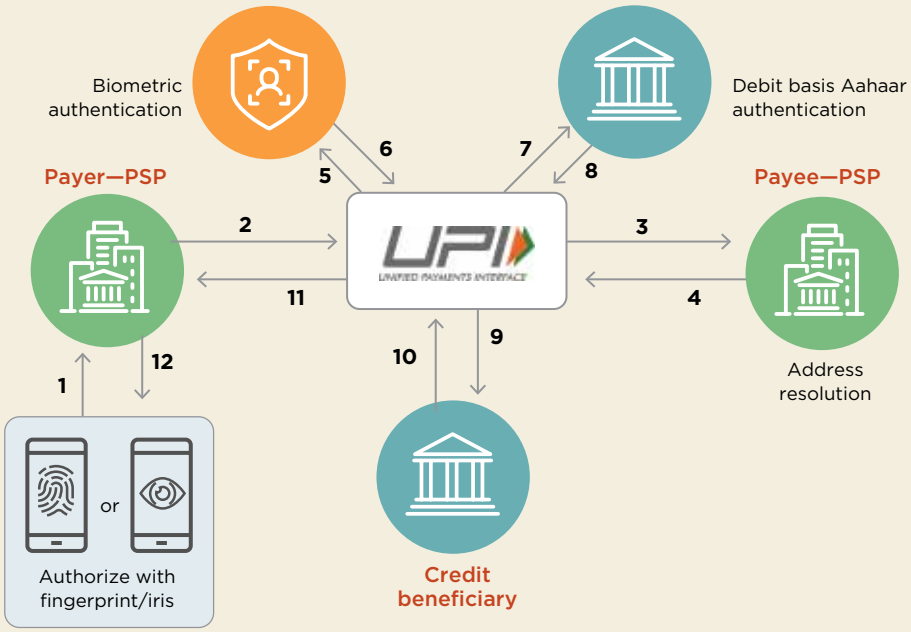
UPI provides a standard set of APIs to enable transactions on UPI platforms, thus enabling a fully interoperable system across all banks, financial institutions, and payment systems without having silos and closed systems. These fully functional APIs allow innovative PSPs to build customized payment solutions for businesses and functionality-rich mobile apps for consumers without having to change the core API structure. UPI uses one-click two-factor authentication for safe and secure payment using a personal mobile phone without the need for any separate acquiring devices or physical tokens.

Businesses could collect payment from customers through UPI or via a QR code. Customers can choose

continued

from various UPI mobile apps to pay through the UPI system and by the BHIM app, which was developed by the National Payments Corporation of India as a government-supported digital application. Popular apps, such as Google Pay (earlier Tez) and PhonePe, launched their own apps on UPI, as did several key banks (such as SBI's YONO). Payment gateways such as Razorpay enabled acceptance via UPI and set it as the default payment mode.

FIGURE 14: UPI Sample Interfaces



Source: Scroll.in[74]

In Australia, the Payments System Board of the Reserve Bank of Australia decided to undertake a "strategic review of innovation in the Australian payments system" in May 2010. The purpose of this project was to identify areas in which innovation in the Australian payments system might be improved. The conclusion of the "strategic review" included the need to establish a FPS system. The key strategic objectives laid out by the reserve bank for the New Payments Platform were to receive low-value payments outside normal banking hours, to send more complete remittance information with payments, and to address payments in simple manner. The New Payments Platform faster-payment system was launched in February 2018. The system enables instant payments between bank customers and other financial service providers and can be used to send money to one or many recipients. Final settlement of funds transferred between banks occurs in less than one minute using the reserve bank's Fast Settlement Service. Individuals who wish to transfer funds to other individuals do not need to know the recipients' account information because the New Payments Platform maintains proxies for bank accounts, which can include email addresses or telephone numbers. Messages are sent on a peer-to-peer basis among financial institutions, while a copy is sent to the Reserve Bank of Australia for settlement. The New Payments Platform depends on the SWIFT Network for sending messages and uses the ISO 20022 message format.

In the United States, the Clearing House (TCH) launched its Future Payments Initiative in 2014 based on the recommendations from its supervisory board, which consists of several industry leaders from financial institutions. The initiative's aim was to develop a strategic view of real-time payments based on an extensive study of payment needs in an increasingly digital economy. TCH worked closely with industry associations, including the Federal Reserve, National Automated Clearing House Association, American Bankers Association, Independent Community Bankers of America, National Association of Federally-Insured Credit Unions, and Credit Union National Association, as well as TCH banks, to identify consumer and business cases with the greatest need for real-time payments that represent the best incremental value for customers. The Future Payments Initiative considered the experience and lessons learned from other countries that had already established their own real-time payment system. TCH also reviewed ways in which a potential real-time-payment system for the United States could maintain and improve the safety and soundness of existing payment systems. The Real-Time-Payment system was eventually launched in November 2017, and it is faster than conventional payments, supports only credit-push transactions, settles payments on a 24/7 basis, and settles on the payee account seconds after making the payment. It is designed to address unmet customer needs across all customer segments (business to business, business to consumer, consumer to business, P2P, account to account, government to citizen, and so forth). Consumers, businesses, and the government can use the Real-Time Payments network.[75]

In Europe, the Single Euro Payments Area (SEPA) Instant Credit Transfer scheme was launched in 2017 to allow instant credit transfers across the pan-European region. According to the European Payments Council, funds transferred using the SEPA Instant Credit Transfer scheme are delivered within 10 seconds. Fifteen countries had signed up for the program by 2018. Other countries are in the process of signing up for the scheme, with a goal to make it the primary solution for instant payments across the European Union.

9.5 RECOMMENDATIONS

- In case there are economies of scale, the regulators should encourage the market to establish an FPS-based clearing-and-settlement platform for domestic payment transactions.
- A faster payment system should be developed with future market expectations in mind, including access to non-bank PSPs and integration of EPA; bill payment; government payment; access to mobile, card, and bank accounts; and other perceived services. Additionally, owner/operators should ensure FPS implementations to account for the following benefits of such systems:
  - Cost efficiency for instant credit transfers
  - Ease of acceptance for merchants and consumers utilizing QR codes
  - Use of financial-management tools by merchants to improve understanding of consumer behaviors/patterns
  - Use of fraud-management tools, especially for e-commerce merchants
  - Use of APIs to build overlay services for merchants and individual payers
  - Integrate additional services, such as request to pay, which is particularly relevant for merchants, as it can help with liquidity management and reduce the cost of collecting debt and payments from customers

Service providers should seek to settle funds on merchants' accounts on a real-time or near real-time basis. Merchants should be able to use the funds received from their clients on an immediate basis either to purchase new goods or services or to accrue their profits.

10. Concluding Remarks

As elaborated throughout the report, innovations in EPA are arising at all stages of the EPA process and through the use of diversified tools, technologies, and business models. Both traditional payment instruments, such as cards, and new ones, such as e-money and e-wallets, are witnessing innovations. One of the major success factors for these innovations is how they add value to all stakeholders participating in the EPA value chain.

Developing EPA is a multidimensional process in which each stakeholder has a role to play. While process efficiency, profitability, business sustainability, and customer loyalty are key drivers for financial institutions and service providers, the interests of other stakeholders, including merchants and customers, are also core to the process and should be considered and protected.

Merchant interests and needs are important considerations for EPA implementations to succeed. Merchants need to see value to their businesses resulting from accepting electronic payments—the growth of their business through a diversified consumer base, safety and security, the time it takes to receive funds, and how much it costs. EPA methods should be tightly linked with the merchants' day-to-day business, providing immediate access to funds, enabling the use of collected funds to procure goods from their suppliers, extending credit to merchants, and minimizing the fees of EPA.

Since payments is a two-sided market and customers are the ones who make the initial decision on how to pay, customers should be incentivized to pay electronically. Programs such as cash-back rewards, hardship and installment, or redeemable points on usage are always strong incentives for usage. However, the impact of those programs could be temporary unless they establish a sustainable habit of using cards, e-money, or e-wallets for big and small day-to-day purchases. By linking a payment instrument to a salary or pension program that replenishes the account automatically on a regular basis, enabling remote access to the account through the internet or mobile phones, and enriching the use cases available to customers, more users will turn to the e-payments as a convenient way to make payments.

Regulators can also fast-track innovations in EPA by improving the enabling environment for retail payments that allows new business models, products, technologies, and service providers to evolve on an even playing field. Regulators should focus on risks and develop proportional regulations that aim at risk mitigation. Regulators need to develop regulations that target policy objectives, such as financial inclusion, interoperability, market competitiveness, and consumer protection. This report addresses many aspects related to regulations, including simplified due-diligence guidelines for merchants, estab-

lishing a level playing field for providers, and avoiding market fragmentation.

During the preparation of this report, the world was struck by the COVID-19 pandemic. The pandemic underlined the importance of EPA, as social-distancing measures were implemented and it became necessary to shop and pay remotely. Many countries took measures to ensure the smooth flow of goods and services, especially those that were important and strategic, during the pandemic. Regulators implemented the following measures to facilitate electronic payments during these unprecedented conditions:

- Facilitating the use of digital payments and ensuring the availability of digital payment services through measures such as reducing or waiving fees on electronic payments, raising limits on electronic transactions, and campaigning and marketing for the use of e-payments.
- Expanding the issuance of electronic-payment instruments, such as cards and e-money accounts through government social-protection programs, to reach out to the maximum number of beneficiaries within the country. Regulators took extensive measures to facilitate the issuance of cards and e-money accounts to vulnerable groups via financial institutions and service providers. Some measures waived the fees of opening new accounts.
- Simplifying customer and small business due-diligence processes: By issuing guidelines to simplify the requirements for enrollment, many central banks facilitated remote enrollment in financial services by accepting a photo of the national ID card while waiving or postponing the mandate of a physical check, and by relying on third-party data such as mobile network operators or national identity databases for information verification.
- Expanding the access points through subsidized plans to acquire small and medium-sized merchants in the acceptance schemes. Plans included providing subsidized POS terminals and other acceptance-related accessories and expanding the use of NFC-based payments and those based on QR codes. In many cases, this was supported by free enrollment in national social-protection programs associated with the distribution of cash or food programs through the enrolled local merchants and agents. Many authorities considered the agents as "essential business" and allowed them to operate to ensure proper delivery of cash to different areas in the jurisdictions.
- Accelerating the development of payment infrastructure: Where interoperable platforms such as FPS, automated clearing houses, and domestic switches were already in operation, many authorities recognized the impact that such infrastructure could have on the digitization of government payments and collections streams and the smooth circulation of cash under such conditions. Authorities expedited the development and enhancements of infrastructure to make the best utilization of all available channels.
- Enhancing operational aspects by extending the operating hours of payment systems and services, enhancing business-continuity arrangements, including disaster-recovery sites, and taking measures to mitigate cybersecurity risks. Both regulators and financial service providers are working to ensure that the payments and financial market infrastructure will continue to work promptly and bear the new loads of utilization caused by newcomers and extensive usage of payment services.

Finally, this report aims at opening new horizons in EPA by showcasing different types of innovations in business models, regulations, and technical instruments. Although the report focuses on existing trends in payment innovation, there is an attempt to focus on general aspects of business models and regulatory measures that would boost EPA. Our target is to enable better opportunities for the estimated 180 million MSMs in developing countries to have access to finance and to allow their 4.5 billion daily customers to use electronic payments.

APPENDIX A

Principles of Developing a Risk-Based Approach to the KYC Process

Undertake a risk assessment. The starting point for designing the system is to identify the main money-laundering and fraud risks and to assess the risk in relation to the services offered and the merchant types involved.

Categorize the different types of merchants to be assessed. Different categories of businesses may have different risk profiles.

- Consider the merchants' geographical location. Businesses in one part of a country may have a different risk profile than similar businesses elsewhere.
- Consider the nature of the business. Are there types of businesses that are more or less likely to be targeted for criminal abuse? Businesses associated in that country with organized crime would generally have a higher exposure to the threat of abuse.
- Consider the most important threats that micro merchants would face, including the likelihood that
  - Criminals would decide to abuse a merchant, rather than a financial institution or gambling institution, which are often attractive targets for such abuse; and
  - Criminals would elect to launder money or finance terrorism using a micro merchant, rather than a large merchant dealing in high-value goods.

A September 2017 report by IFMR LEAD, *The Evolving Financial Ecosystem for Micro-Merchants in India*, studied attributes of micro merchants in five cities in India. The businesses operated in the following categories: garments, medical stores, kirana stores, food and beverage outlets, consumer electronics, mobile phones and accessories, automobile accessories and spare parts, buildings and fittings, men's salons or barbers, beauty parlors, watches and accessories, and private cabs.

Of the 547 micro merchants surveyed, 83 percent were sole proprietorships, 13 percent were owned by a household, and 4 percent were partnerships. The mean number of employees was 2.83, and the enterprises reported average monthly sales of about $1,300 for the period May–June 2017. The size of the businesses differed by location. Monthly sales, for example, ranged from just over $200 for micro merchants in one city to more than $3,200 for those in another city. A risk assessment of merchants would ideally take differences in business size, the nature of the business, and location into account.

Design appropriate due-diligence measures. Effective, efficient, and proportional risk-mitigation measures must be designed for the different types of merchants and the different risk levels identified. These measures are intended (i) to identify and verify the identity of the customer and beneficial owners, allowing for sanctions and other screening processes to be followed; and (ii) to profile the customer to enable transaction monitoring.

Be reasonable and pragmatic about identity verification. AML/CFT rules require the customer to be identified and, generally, for the identity to be verified. FATF is not prescriptive about how that should be done. Identification is aimed at uniquely distinguishing the customer from all other potential clients. For natural persons, that often means recording a person's full name, gender, date of birth, and/or any unique identifying number, such as a national ID number, where issued. Not all of this information needs to be verified, but when required, sufficient details should be verified to provide assurance that the person is who he or she avers to be. Verification can be against a document, such as a national ID card or a letter from a community leader, or against data, such as the national ID database. It is, however, crucial to be pragmatic and not to require documents that a large section of the customer base would not have.

Verification itself, however, is optional under the risk-based approach where risks are assessed as low in the national risk assessment. This option can be exercised by a financial institution only if allowed by the regulator.

Take reasonable steps to identify beneficial ownership. A beneficial owner is a natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted, and/or those persons who exercise ultimate effective control over a legal person or arrangement. Institutions must take reasonable measures to verify to their satisfaction the identity of the beneficial owner. For legal persons and arrangements, this should include financial institutions that understand the ownership and control structure of the customer. In the case of micro merchants, businesses are generally sole proprietorships or family owned.

Collect contact particulars. It is standard procedure to ensure that customers can be contacted. Residential and business postal addresses and web addresses may, therefore, be recorded, but email addresses and mobile phone numbers may prove to be the most practical means of contacting customers. These are often also the most relevant details for virtual businesses that operate in cyberspace with no physical offices or physical addresses.

Collect profiling information. Profiling information is the information required to understand the business of the customer. How does the customer earn an income? If the customer is a business, what is the type of business? Where is it conducted? Who controls the business? Who manages the business? Who has the authority to represent the business? Profiling information supports transaction monitoring, and such monitoring is ultimately one of the best ways to identify any unusual activity. Importantly, FATF profiling information does not need to be verified, as the monitoring of business transactions provides the best means to identify potential criminal abuse of the relationship.

Be pragmatic when verifying micro merchants. Micro merchants refer to very small businesses, such as street vendors, barbers, or tuk-tuk drivers. It is important to broaden the payment system to include the typical transactions that the poor conduct in cash every day. These businesses are very small and informal but provide important services to low-income people.

These businesses are generally sole proprietorships belonging to one owner or a family. They are not incorporated companies and therefore lack state documentation issued upon the incorporation of a business. They would often not have a registered name. Identification and verification of the business and the beneficial owner in these cases would focus on the identity of the individual(s) owning the business. Requirements for the identification and verification of individuals, therefore, are a key part of MDD rules.

In addition, careful thought must be given to the verification processes. In countries with a national ID system, it may be easy to use the national ID card or data to verify the individual. That should suffice, unless there are business-related documents that the particular type of business can be expected to have—for example, a driver's license or vendor license, in which case that may also be requested. License requirements, however, may differ from city to city. MDD rules should not be unduly rigid, requiring documents that may be available to some but could not reasonably be expected of all merchants.

Endnotes

1. According to the World Bank's definition, micro businesses have between 1 and 9 employees, while small businesses have between 10 and 49 employees working in the same location. *Merchants* refer to retail providers who sell goods and services. Despite the reference to MSMs, many areas of the report focus on micro merchants.
2. It should be clear that in some environments where the traditional model is well developed and adopted by MSMs (for example, Brazil), such models are still preferred over emerging ones and will continue to evolve as long as they add value to all stakeholders and create balance among the relevant parties.
3. The report discusses an illustration of major stages in the acceptance process.
4. Global Development Incubator and Dalberg, *Small Merchants, Big Opportunity* (Visa, 2016).
5. Same reference.
6. The report uses the terms *payment facilitator*, *payment aggregator*, and *merchant aggregator* interchangeably.
7. In 2018, EMVCo created a QR Payment Mark to promote global interoperability across EMV QR code payments. It developed reproduction requirements and a free licensing structure to enable all implementers of EMV QR code solutions to use the mark.
8. All merchants who accept payment cards from international schemes must comply with the Payment Card Industry Data Security Standard (PCI-DSS).
9. *Innovation in Electronic Payment Adoption: The Case of Small Retailers* (World Bank Group, 2016) and *Building Electronic Payments Acceptance at the Base of the Pyramid to Advance Financial Inclusion* (Mastercard, 2018).
10. In a closed-loop system, the relationship is typically between the merchant and merchant bank, and no processor is involved. Merchant banks provide the hardware and software to the participating merchants, and the payments are more of an internal process than when accepting outside electronic payments. Closed-loop payments can also frequently be made on propriety apps or mobile-payment solutions.
11. These incentives could be built into the sales contracts of the DSAs and are typically paid through the merchant discount rate.
12. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/
13. Mobile Money for the Unbanked (GSMA).
14. *State of the Industry Report on Mobile Money* (GSMA, 2017).
15. First Data, Secure Global Pay, and Law Insider websites.
16. Square, Mastercard.
17. Mastercard mPOS case study.
18. "mPOS Best Practices," available at https://mpos.mastercard.com/_assets/pdf/Mastercard%20MPOS%20Food%20Truck%20Case%20Study%20ENG.pdf.
19. Ant Group Services.
20. Some exceptions to the above statement include NFC-based wallet transactions. Some QR solutions are considered card-present transactions.
21. FIS Global blog.
22. Global Development Incubator and Dalberg, *Small Merchants, Big Opportunity* (Visa 2016).
23. *Innovation in Electronic Payment Adoption: The Case of Small Retailers* (World Bank Group, 2016).
24. The Swedish company Klarna and the Australian company Afterpay are market leaders in providing POS installment loans. PayPal has recently launched "buy now, pay later" products in the United States and United Kingdom called "Pay in 4" and "Pay in 3," respectively, that allow consumers to finance their purchases over three interest-free monthly installments.
25. "Mobile Money Pricing" (CGAP website).
26. FATF, "GUIDANCE Anti-Money Laundering and Counter-Terrorist Financing Measures and Financial Inclusion," 2017, 45-52.
27. FATF, GAFILAT, "Anti-Money Laundering and Counter-Terrorist Financing Measures, Mexico, Mutual Evaluation Report," 2018, 38.
28. FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation," 2012, 30.
29. FATF, same reference, 2012, 64.
30. FATF, same reference, 2012, 64.

31. FATF, same reference, 2012, 64.
32. FATF identifies casinos, trust and insurance services, and dealers in precious metals and stones as high-risk businesses.
33. http://www.sbp.org.pk/bprd/2019/C5.htm
34. Computerized National Identity Card.
35. National Database and Registration Authority.
36. By the United Nations Security Council's list of entities and individuals proscribed under Schedule I and Schedule IV of the Anti-Terrorism Act, 1997, respectively, and any other applicable sanctions lists.
37. In comparison to payment cards, mobile-money services do not have the same types of credit risks.
38. WorldPay Payfac tools and services, PayJunction merchant underwriting.
39. Risk underwriters also look for frequently changing or attempting to change merchant processors; specific merchant risk categories such as collection agencies; other merchant businesses reported on the same bank account statement; financial instability; a main source of revenue coming from another business; or sharing an account with another merchant. In high-risk underwriting, there is no standard risk criteria to follow, as not all merchants are the same and the level of risk and required due diligence may vary.
40. Trulioo best practice merchant onboarding.
41. Visa Global Risk Standards/Paysimple merchant account underwriting.
42. Trulioo/Provonir website.
43. https://www.mckinsey.com/business-functions/risk/our-insights/new-credit-risk-models-for-the-unbanked
44. "Rethinking Credit Lending" (Infosys).
45. "Alternative Data Transforming SME Finance" (IFC, 2017).
46. By the first quarter of 2020.
47. PayPal US and PayPal reviews in *Merchant Maverick.*
48. Ant Group.
49. European Central Bank, "Oversight Framework for Card Payment Schemes: Standards," January 2008.
50. This example is hypothetical and meant for explanation only.
51. Capgemini, *Domestic Payment Card Networks: Emerging Opportunities and Challenges, 2017.*
52. Paymentafrica.com.
53. EMVCo website.
54. https://www.emvco.com/emv-technologies/qrcodes/
55. Mobile Money: Africa's Other Mobile Money Juggernaut (CGAP).
56. Global Knowledge blog on multifactor authentication, 2018.
57. Visa and Securion Pay websites
58. Mastercard Secure Code
59. EMVCo website
60. "EMV Payment Tokenisation," available at https://www.emvco.com/emv-technologies/payment-tokenisation/.
61. "Registered IDs," available at https://www.emvco.com/approved-registered/registered-ids/.
62. Storing payment card information on a computer or mobile phone is referred to as card on file.
63. Payments Journal.
64. https://medium.com/rivero-ag/7-things-every-issuer-and-bank-should-know-about-the-secure-remote-commerce-src-7a49a7842c89
65. Prepaysolutions Virtual Card Numbers, Conferma Banking White Paper, Credit Card insider.
66. https://nppa.com.au/
67. Subject to a low threshold, https://business.paytm.com/pricing.
68. FIS Global Report.
69. "Small Merchant Digital Financial Inclusion" (Mastercard website).
70. FIS Global Report, Deloitte Consolidating Real Time Payments Report.
71. Committee on Payments and Market Infrastructures, *Fast Payments—Enhancing the Speed and Availability of Retail Payments* (Bank for International Settlements, November 2016).
72. http://pubdocs.worldbank.org/en/449461608572673957/FPS-Preview-Report-WB-Dec-17.pdf
73. Razorpay website and CCAvenue UPI.
74. https://scroll.in/article/850371/smartphone-users-could-soon-make-transactions-using-aadhaar-linked-fingerprints-reveals-paper
75. "RTP," available at https://www.theclearinghouse.org/payment-systems/rtp.


THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP


EUROPEAN CENTRAL BANK