TECHNICAL NOTE

CGAP

STARTING THE TRANSACTION: PAYMENT INITIATION AND CUSTOMER EXPERIENCE

April 2023

William Cook, Dylan Lennox, Souraya Sbeih

Consultative Group to Assist the Poor
1818 H Street NW, MSN F3K-306
Washington DC 20433
Internet: www.cgap.org
Email: cgap@worldbank.org
Telephone: +1 202 473 9594

RIGHTS AND PERMISSIONS

Contents

EXECUTIVE SUMMARY

INSTANT PAYMENT SYSTEMS facilitate the various types of small-value, mobile payments most frequently used by low-income customers. However, speed and availability are only part of what makes these systems work better for the poor; they are also increasingly fostering a simpler, more intuitive user experience.

It is payment initiation—the first step of the transaction—that dictates exactly how well this user experience will work for low-income customers. In simple terms, payment initiation is the start of a transaction. For card-based payments, this has traditionally meant tapping or swiping a piece of plastic. For instant payments, the experience is more often mobile, and a dizzying array of tools is being developed to help make the process more intuitive for customers.

From standardized QR to third-party initiation to Request to Pay, these tools each have value to add, but their number and complexity can make it difficult for policymakers and system operators to prioritize. It is also hard to establish which of them work best to improve outcomes for poor people.

This technical note is framed to help policymakers and payment system operators understand recent trends in payment initiation and prioritize the solutions that will make the most difference to the customer experience among low-income populations. It finds that:

- *Adoption of alias-based addressing offers an important opportunity to reduce complexity and increase consumer protection in the use of mobile payments.* However, directory design choices offer trade-offs between data protection, flexibility of alias, and time/cost of implementation, and so should be weighed carefully.
- *Trends in QR standardization are improving the usability of QR-based payments for the smallest merchants.* Yet the paths taken to standardization differ between markets, and the fastest route to scale can depend heavily on market structure.
- *Third-party payment initiation can be invaluable in expanding the provision of instant payments beyond traditional actors*. However, the timing of implementation and underlying economic models must be carefully considered, as the potential to disrupt existing services already serving poor people is high.
- *Request to Pay services can help lower the digital/financial literacy burden placed on consumers in initiating a transaction.* The most forward-looking solutions are offering opportunities to also improve data-sharing and customer redress. Though as with other solutions described here, fit-for-purpose design and implementation are critical.

The paper concludes that while instant payment systems play an important role in supporting a shared customer experience, the private sector's ability to differentiate individual products is also critical. Policymakers and system operators should balance competition and coordination—promoting a shared language for instant payments while also not limiting the private sector's ability to stand out from peers.

INTRODUCTION

INSTANT PAYMENT SYSTEMS—ALSO known as fast, immediate, or rapid payment systems— facilitate the types of small-value, mobile payments most frequently used by low-income customers. These systems offer continuous, real-time availability, allowing financial transactions between providers to be completed within seconds at any time of day or night.

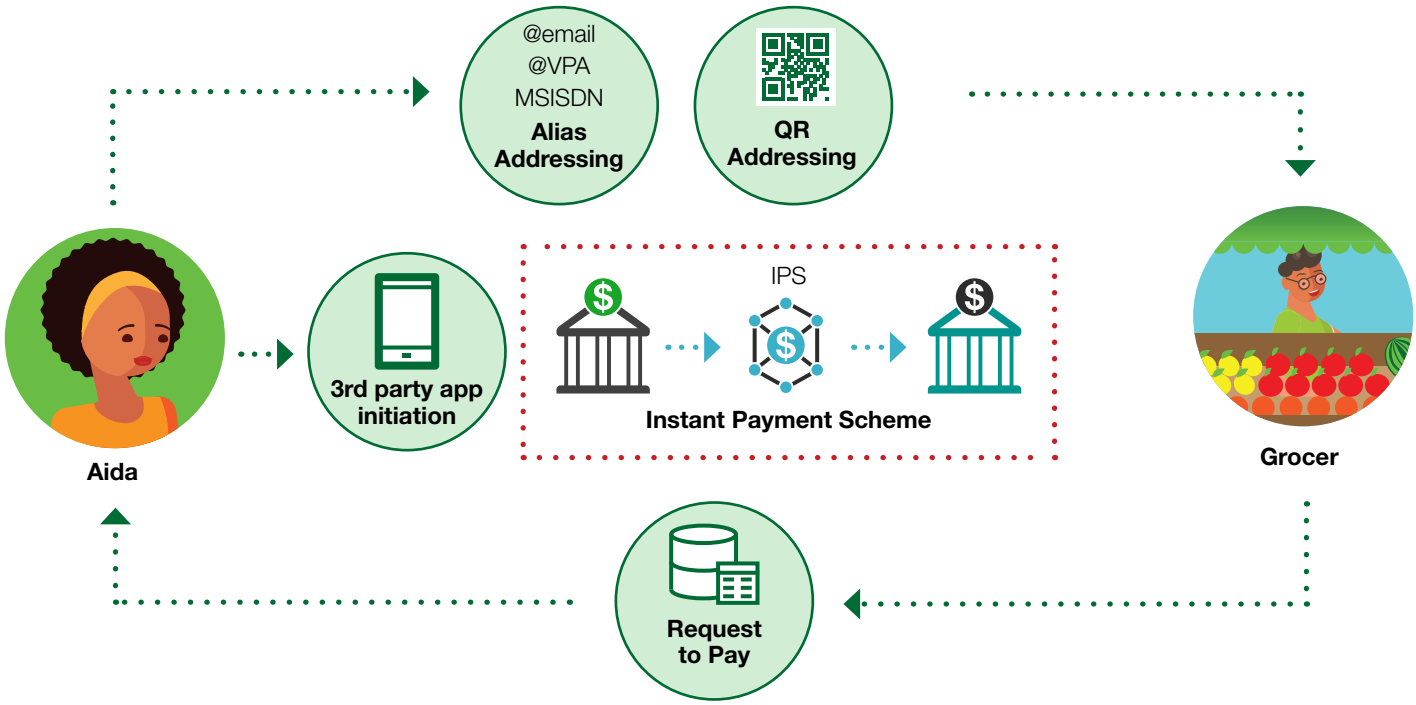
However, speed and availability are only part of what makes them work better for the poor. Instant payment systems typically facilitate a simpler, more intuitive user experience. This experience is predominantly mobile, and increasingly tailored to customer needs through innovations such as alias-based addressing and third-party initiation.

Effective clearing and timely settlement are prerequisites to safe and efficient transactions, but it is payment initiation—the first step of the transaction—that often dictates much of the experience a customer has while making a payment. As a result, decisions made by a scheme related to payment initiation can make or break the customer experience.

This technical note is framed to help policymakers and payment system operators understand recent trends in payment initiation and prioritize the solutions that will make the most difference in customer experience for low-income populations.

The note builds on the CGAP technical guide Building Faster Better: A Guide to Inclusive Instant Payment Systems (Cook, Lennox and Sbeih 2021).

FIGURE 1. **Recent trends in payment initiation customer experience**



WHAT IS PAYMENT INITIATION?

IN THE SIMPLEST TERMS, PAYMENT initiation is the start of a transaction. Initiating a payment, as with sending a letter or an email, requires knowing at least two things: an address and a message. For a digital payment, this means identifying an account (source or destination) and the amount to be paid.

The message may also include details required for authentication such as a PIN code, or additional information such as an instruction to make the transaction recurring, but it will always include a payment address and amount.

Consider a customer paying at a market for fresh apples and oranges. This customer (let's call her Aida) might use either a debit card from her bank or scan a QR code to make an instant payment from an app. Either way, Aida quickly pays for the fruit and walks out happy. In both cases, Aida's identity is authenticated, there is a debit and a credit, and confirmation messages are exchanged in near real-time. One could then be forgiven for thinking that when comparing those two means of payment we are comparing apples with apples. If you look a little more carefully, you will see that her card and instant payment transactions are more like apples and oranges.

In a traditional card, or 'pull', transaction the process begins when Aida hands over her card details. As shown in Figure 2, the merchant captures Aida's address (the card number) and the payment amount, asks Aida to

FIGURE 2. **Initiation of a card payment (pull transaction)**

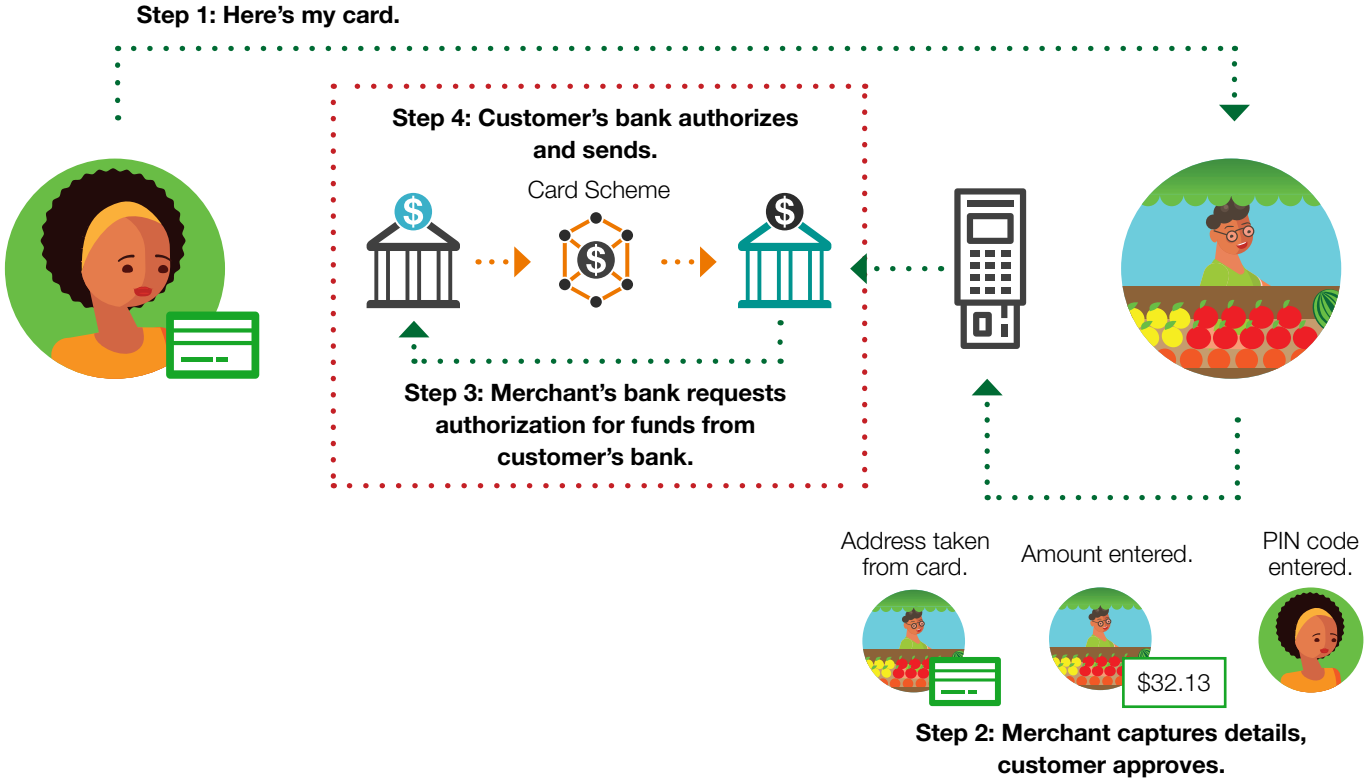
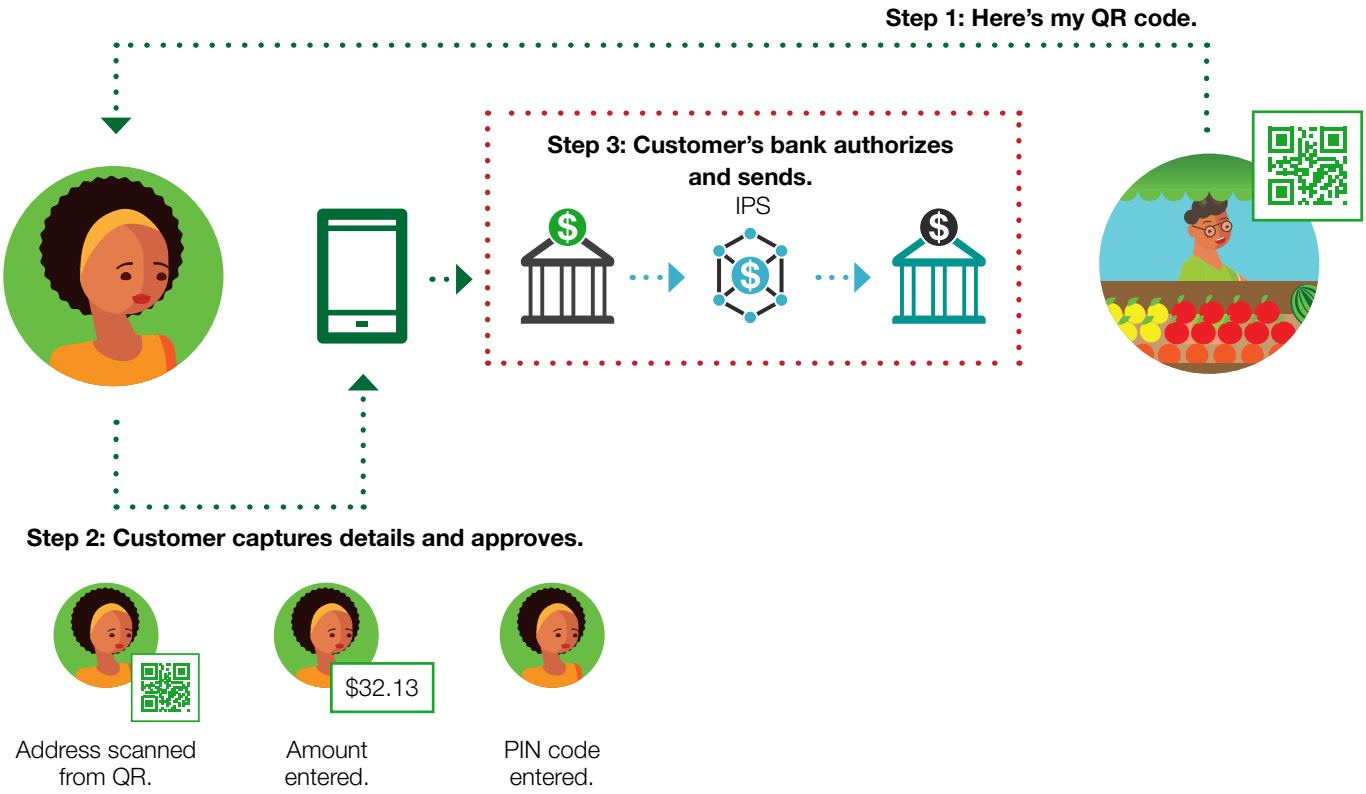


FIGURE 3. **Initiation of an instant payment (push transaction)**



authenticate herself, and then sends a request (via the merchant's bank) for Aida's bank to transfer the funds.

With instant payments (and any form of 'push' or 'direct credit' payment, such as a wire transfer), the same information needs to be shared, but the process is reversed. As shown in Figure 3 the merchant will provide Aida with the address for the payment and the amount due, and then Aida will ask her bank to make the payment.

Why does this difference matter? First, the form of payment (push or pull) can dictate things like how quickly the receiver (e.g., merchant) gets access to the funds, the liability for the bank, and by extension, the cost of the payment. But more relevant for our purposes, push and pull transactions ask very different things from the customer experience.

The pull scenario required Aida only to hand over her card, while the instant payment required her to input multiple pieces of information. Many of the innovations in initiation for push payments (things like QR codes and Request to Pay services) are responses to this fundamental difference. This note focuses on the actions schemes and regulators are taking to make it easier for Aida to perform an instant/push payment.[1]

1 While the focus of this note is on 'instant payments' – those mobile payments primarily used by lower income customers in developing markets, it should be noted that much of the same innovation is happening today in card systems, leveraging tools like card tokenization.

FORMS OF ADDRESS

PAYMENT INITIATION INVOLVES sharing at least two pieces of information—an amount and a payment address. But what is a payment address?

To her bank, Aida is a number (in addition to being a valued customer, of course). Aida will be identified on her bank's system by an account number, often randomly generated, unique to her.

At the payment system level, her bank will be similarly identified by some sort of unique number – a routing number or bank identification code (BIC). Anyone who has registered their bank account for a direct deposit service or sent a wire transfer has likely seen both numbers before.

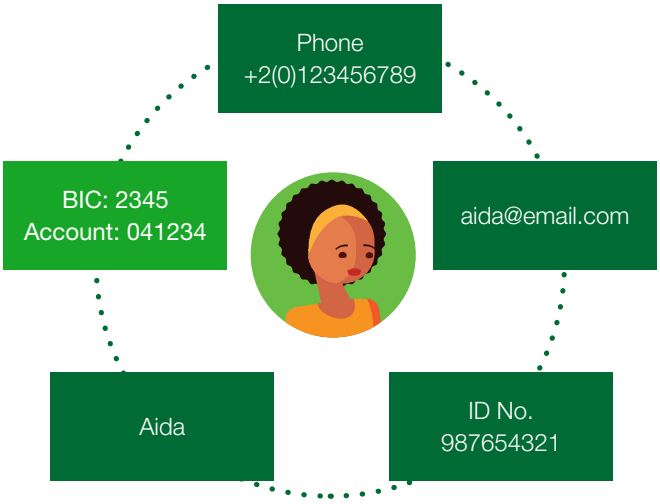
However, remembering long account numbers and routing codes is inconvenient. It is even more inconvenient as digital payments become used for more everyday transactions.

Many instant payment systems now use alias-based addressing to help identify senders and receivers. Account numbers still exist behind the scenes, while aliases just provide another, simpler, way to identify the account. Aliases can be almost anything—phone numbers, user names, email addresses, ID numbers, or temporary codes (e.g., for online transactions). See Figure 4.

The idea of an alias is nothing new. Closed-loop, non-interoperable products have used them for years. Mobile money products like M-PESA in Kenya and bKash in Bangladesh use phone numbers to identify customers (and till numbers for merchants). Products like PayPal have linked accounts to email addresses since the early 2000s.

An alias must be unique within the scheme. Just as a product like M-PESA cannot have the same phone number representing two different accounts, neither can an alias represent different accounts within the scheme. Uniqueness within a scheme needs to be managed somewhere, and this can be done through either a centralized or a decentralized approach.

FIGURE 4. **Examples of forms of addresses**

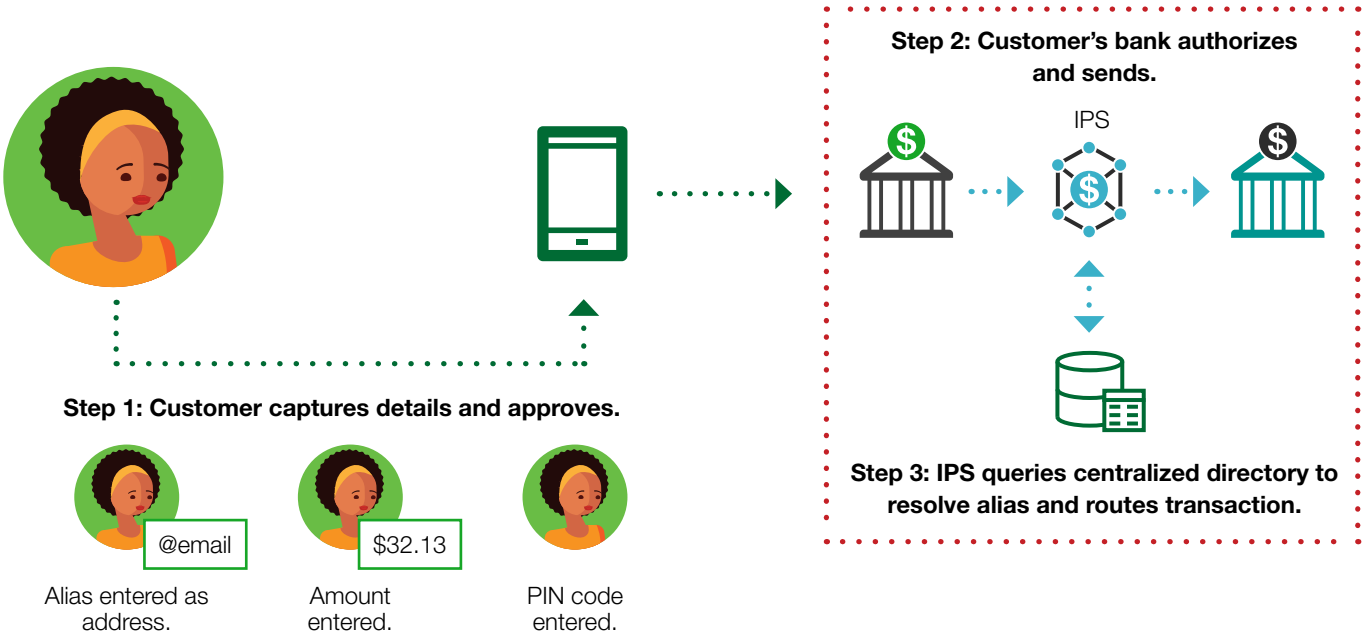


Centralized directories

A centralized directory operates exactly like its closed-loop predecessors, only at the scheme level. A single directory (like a phone book) sits with the payment system operator and links each alias with a given financial institution where the corresponding account is held. See Figure 5.

A centralized directory allows for flexibility in the type of alias used, and system operators are increasingly taking advantage of this flexibility to give users more options. For example, Pix in Brazil allows an alias which

FIGURE 5. **Instant payment transaction using an alias based on centralized directory**



Centralized Directory Service

Forms of address	Advantages	Disadvantages	Examples
Any alphanumeric (e.g., phone numbers, email addresses, nicknames)	Flexibility for customers; users can choose an alias using an existing identifier which is well known (e.g., email address).	Higher capital investment and processing overhead at scheme level. Increased cybersecurity risk where account information held in single repository	PesaLink in Kenya PayM in UK PayID in Australia Pix (DICT) in Brazil

can be a mobile phone number, an e-mail address, a Taxpayer Identification Number, or even a randomly generated alphanumeric.

Compared to decentralized solutions, a centralized directory is more complex in terms of technical implementation at the scheme level. A high-speed and high-availability database containing the aliases must be added to the payment system operator's infrastructure and this database must be maintained over time.

APIs and messaging standards must also be adopted by each participant to allow them to add, edit or remove aliases from the central directory. The cost of operational capacity for these activities (alias management and resolution messaging) add to the overall cost of transaction processing for the scheme.

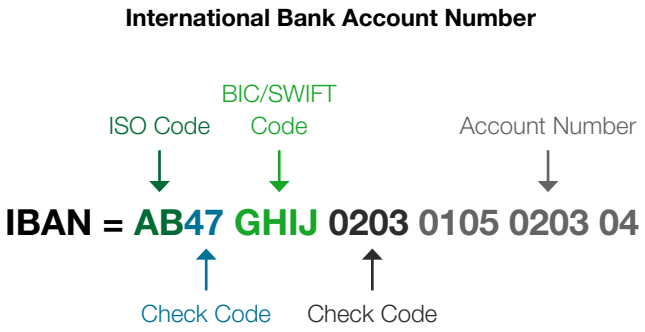
Decentralized directories

Decentralized directories involve financial institutions maintaining the link between the alias and the account within their system. The scheme only helps in determining where to pass the message for address resolution.

Traditional bank accounts and routing codes are an example of this arrangement, as is IBAN, the internationally agreed standard of identifying bank accounts across borders. As shown in Figure 6, the various components of the IBAN tell the payment system operator where to send the funds.

In the instant payments world, standards similar to IBAN could be agreed within the scheme, but these would be difficult to communicate for everyday payments. In India, UPI's virtual payment addresses (VPA) instead use a

FIGURE 6. **Example of decentralized addressing – IBAN number**

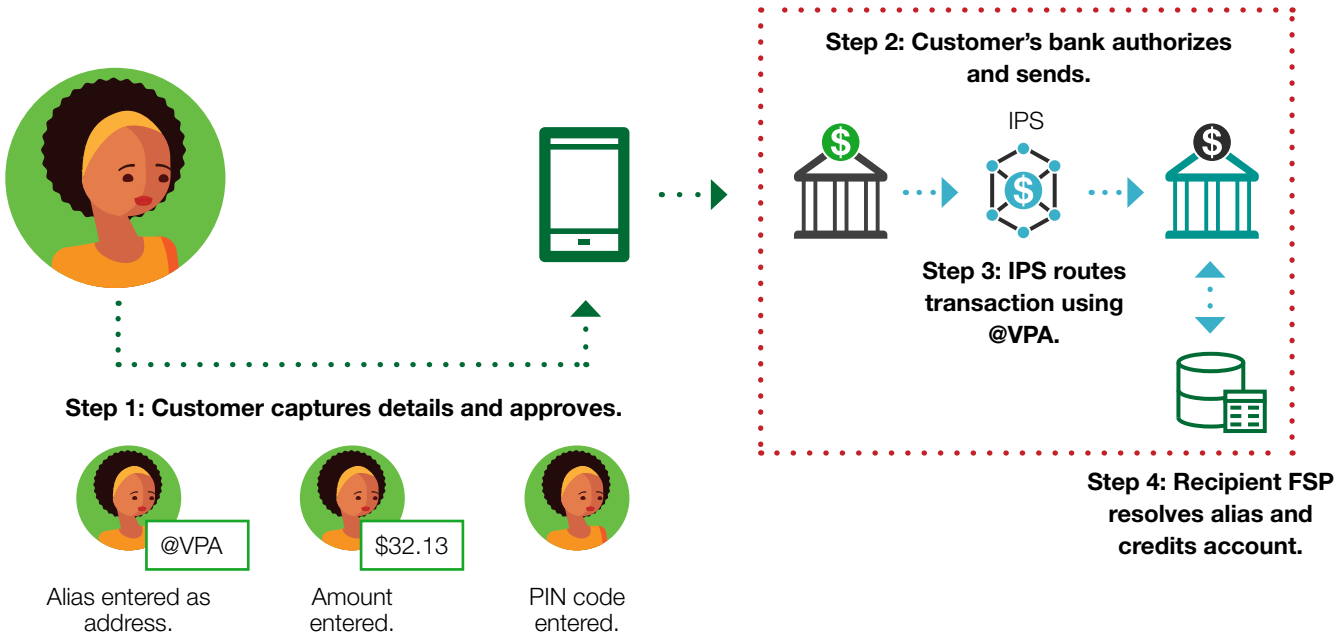


domain-based concept similar to how email is managed, for example: Aida123@FriendlyBank.[2]

The @FriendlyBank domain allows the system operator to determine which participant will be able to decode the account number. The Aida123 allows the address-holder (e.g., Friendly Bank) to locate the correct underlying account. As shown in Figure 7, some type of mapping is still required at the scheme level to determine the right destination.

The decentralized approach provides potential advantages for data protection and cybersecurity—account numbers are not held with the payment system, only with the account provider. A decentralized approach also means less financial investment at the payment system level.

FIGURE 7. **Instant payment transaction using an alias based on a decentralized directory**



Decentralized approaches

Types	Advantages	Disadvantages	Examples
Structured number formats. Domain-based virtual payment address.	Low infrastructure investment needed. Data protection.	Customer must be issued a new alias from their account holder within the standards and availability. Participants may need to upgrade systems to manage the alias.	IBAN UPI India

2 India also uses centralized directories for accounts identified by Aadhaar ID and for accounts identified by phone number.

Managing directories – the importance of add, change, delete

Whether using a centralized or decentralized directory, the fundamental benefit to Aida is the same. We have allowed her to identify herself by something easier to remember for everyday transactions.

However, financial lives are fluid. Aida may form new accounts, change banks, or end relationships over time. Directory processes must be designed to accommodate these actions safely and efficiently. If not, alias services—designed to make transactions easier—can inadvertently limit customers' ability to change or leave providers. These impacts are most acute for those with the least financial and technical literacy.

Clear, consent-based processes for customers to register, reassign, and remove aliases are important. In Jordan, the JoMoPay system initially implemented a directory based on phone numbers. Because many banked customers already had phone numbers registered with banks, some banks took the step of automatically enrolling their customers in the directory using the phone number on record.

This step by the banks had the effect of blocking some customers from registering for new wallet products, as their alias was already assigned. When attempting to open a new wallet account, these customers learned that their phone number was already assigned to a different provider. To obtain a wallet, customers needed to request their bank to de-register their phone number as an alias. Often, this process could take time to complete.

This story underscores two important lessons for design of directories:

1. **New alias registrations should be performed only with customer consent.**
2. **Removal/de-linking of an alias should have clear processes, with defined minimum service levels such as the maximum amount of time a participant institution can take to submit a change request, once raised by the customer.**

A similar challenge was faced in India. Early on, a feature existed in the Aadhaar Payment Bridge System (APBS) where the registration of a new link overwrote the previous link in the directory. In a well-publicized debacle, a payments bank linked new accounts opened with them as the default for many social protection payment recipients without consent. The welfare payments were redirected into these new accounts without the beneficiary's knowledge (Venkatanarayanan and Lakshmanan 2017).

The India case underscores another important lesson:

3. **Changes to alias, or in the link between alias and account, should only be performed with customer consent and notification should be provided.**

QR CODES AND SHARING TRANSACTION DETAILS

SO NOW AIDA IS NO LONGER LIMITED to a randomly assigned number from her bank. If she is using an alias, she may have options, including an email, username, or phone number. However, when Aida went to pay at the market in our earlier example, she did not enter an account number or an alias. Instead, she scanned a QR code.

A QR code[3] is one example of an encoding technology, a way for the payment address and other transaction details to be more easily shared. In the card world, passing the card number to a merchant is made easier by encoding it in a magnetic strip, embedding it on a chip in the card, or through NFC (tap and pay).

For mobile payments, some of the same forms of encoding are available (e.g., NFC), but the one that is by far the most ubiquitous is the QR code. QR codes—like barcodes in retail or chips on cards—are simply a way to wrap information into something more easily shared.[4]

QR standardization – which model to apply?

As QR codes have become more prevalent, an increasing number of markets are undertaking discussions around QR standardization. The benefits are clear. A single QR standard means that store windows do not have to be covered in the stickers of different providers, and that transactions which may otherwise be interoperable are not prevented by differences in technology.

However, it is important to note that standardized QR codes do not mean that payments using those QR codes are necessarily interoperable. QR standardization is comparable to the readability of EMV chips on cards. The ability of a device to read the information presented is certainly a prerequisite to payments interoperability, but this readability does not mean that the same issuing and acquiring institutions are also connected for passing payments.

There are two broad approaches for standardizing QR codes—scheme-level standardization and market-level standardization—and the difference is important in assessing the trade-offs for QR readability.

SCHEME-LEVEL STANDARDIZATION

Countries like Thailand (PromptPay) and Indonesia (QRIS) have implemented standardized QR codes as part of a merchant payments use case within an existing national scheme. This means that interoperability is implied. As a scheme-based solution, it also means that scheme pricing decisions (e.g., interchange) can be applied across all merchants who accept a given QR standard.

3 To understand more about how QR codes work refer to the blog from CGAP: "Inside QR Codes: How Black and White Dots Simplify Digital Payments" (2017), https://www.cgap.org/blog/inside-qr-codes-how-black-white-dots-simplify-digital-payments.

4 For more information on acceptance technologies, refer to CGAP's guide to acceptance technologies for merchant payments: https://www.cgap.org/research/publication/acceptance-technologies-merchant-payments.

However, the approach has trade-offs. Not all issuers of QR codes in the market are likely to be a part of one and only one payments scheme. At a market level, this means that a scheme-based solution is at best a partial solution. International schemes (e.g., card acquirers like Visa/MCW) and closed-loop providers (e.g., Grab) may still issue their own QR codes to merchants, and the vision of a 'single sticker' will not be achieved.

For Aida, this means that she may be able to pay from her bank account where she sees the 'BankSchemeQR' sticker. But if Aida also has a wallet with MyWallet, which is not a member of the scheme, then she will still need to look for a MyWallet QR sticker in order to pay.

MARKET-LEVEL STANDARDIZATION

As an alternative to a scheme-based approach, countries like Singapore (SGQR) have developed market-level standards to be used within the country by all schemes. A market-level standard has the benefit of creating universal coverage. However, a single standard for multiple schemes means that a given QR sticker/brand does not imply interoperability.

Assume Aida is paying from her same MyWallet account at two different merchants. Each merchant displays a sticker under the brand of MarketQR—the national QR standard agreed by industry and enforced by the regulator. However, one merchant was acquired by MyWallet and the other merchant was acquired by a leading bank, NotHerBank. MyWallet and NotHerBank are not interoperable for merchant payments (not part of the same scheme), and so while Aida sees the same QR code at both merchants, only the MarketQR sticker placed by MyWallet will allow Aida to make a payment.

The above scenario has created a situation in markets like Singapore where a single QR code sticker can be applied, but must specify the participating providers/schemes so that customers know whether they can use the specific QR code to pay. See Figure 8.

Each of these approaches to QR standardization has its advantages, and the right answer for a given market will depend on factors such as the number of schemes and degree of interoperability present in the market. See Table 1.

FIGURE 8. **Example of market-level QR (SGQR in Singapore) (source: Sendingan 2019)**

TABLE 1. **QR codes: market-level versus scheme-level standardization**

	Market-level Standardization	Scheme-level Standardization
Advantages	Merchants reduce the number of QR codes which must be displayed	Payment interoperability implied at the level of the QR, clear recognition of QR brand in market
Disadvantages	Interoperability not certain, potential customer confusion regarding QR brand in market	Merchants have multiple QR codes on display
Context where model is best applied	High level of interoperability exists with multiple schemes operating at scale	A single dominant national scheme has high levels of participation across financial institution types

Box 1. EMV Standards – what goes into a QR code?

Many standardization projects opt to build on EMV (EMV stands for Europay, Mastercard, and Visa, the three companies that created the standard). EMV standards are open and free to use. Their wide adoption has aided harmonization across markets and helped them to stay current in response to issues and persistent threats. But what are the standards?

Essentially, EMV standards are specifications outlining the fields or 'data objects' for QR encoding, also detailing how the data can be organized for most efficient use. The standards provide a wide range of fields, but not all must be used. The list of standard EMV fields includes everything from common data elements such as account address and transaction amount, to fields like loyalty number and purpose of transaction that may only apply in certain contexts.

EMV standards exist for both merchant- and customer-presented scenarios and support both static and dynamic QR codes. They are also generally considered robust, with compliant specifications read by devices in less than a second.

The standards are maintained by EMVCo, a global industry body owned by the major international card schemes (American Express, Discover, JCB, Mastercard, UnionPay and Visa). EMVCo does not provide certification of specific standard regimes, nor does it generally get involved in the implementation of QR standards in specific markets.

Instead, it is up to the payment system (and/or regulator) implementing EMV to decide what parts of the standard are most relevant to local context. For more information on how specific markets have tackled implementing EMV, the GSMA report QR Code Merchant Payments is a helpful tool (Collie et al. 2020). The report illustrates some markets that have adopted EMV, along with which specifications they adopted.

QR codes and protecting the customer

Fraudsters have devised ways to exploit QR codes such as embedding malicious URLs (e.g., used for malware or phishing attacks) or simply replacing legitimate QR stickers with their own to divert a payment to the fraudster's bank account. They may replace a merchant's QR code by swapping it out, or by pasting their own sticker over the existing code.

In the case of a redirected payment, fake accounts must be opened to receive the diverted payments, withdrawn as cash, and then closed, otherwise the fraudulent payments can easily be traced and reversed. As a result, this type of fraud results as much from a failure of customer due diligence as it does from a failure of the QR code.

Even so, there are controls a scheme can adopt to help reduce QR fraud:

- Educating merchants and encouraging them to test that their QR codes are genuine on a regular basis.
- Cryptographic solutions that allow a reading app to be satisfied that the QR code has not been swapped out.
- Presenting the merchants name to the customer through a name lookup function to provide a further checkpoint during the payment initiation process.

There are also privacy concerns with QR codes, and a fraudster could scan a QR with no intention of paying, only to obtain the merchant's account details. However, this threat is reduced through the use of alias-based addressing as discussed earlier in the note.

THIRD-PARTY PAYMENT INITIATION

IN ALL THE PREVIOUS EXAMPLES, Aida was assumed to be using the channel (app or USSD) offered by her account provider. However, an increasing number of instant payment systems are also developing the rules and infrastructure needed to allow her to pay through a financial institution other than her account provider.

Why would anyone want to do this?

Well, say Aida has an account with Old Trustworthy Bank (OTB). OTB is the only bank with a branch in the rural area where she lives—supported by a government financial inclusion initiative. However, the chances that OTB offers the best customer service in the market might not be so great. Third-party initiation breaks the link between user experience (digital channels) and accounts, allowing a customer like Aida to transact from her OTB account using another, perhaps digital-only, provider. See Figure 9.

India's Unified Payments Interface (UPI) is probably the best-known example of a system supporting these services and such third parties have driven much of the transaction volume on UPI. Just two of these services—PhonePe and Google Pay—generated 81% of transactions on UPI during 2021.[5]

The terms for these entities vary. In the European Union, PSD2 refers to them as Payment Initiation Service Providers (PISPs). In India, the National Payment Corporation of India (NPCI) refers to them as "third-party apps". Some jurisdictions include payment initiators

FIGURE 9. **Third party app registration and payment initiation**

5 Calculated on the calendar year of 2021 from NPCI ecosystem statistics: https://www.npci.org.in/what-we-do/upi/upi-ecosystem-statistics.

Box 2. What is the relationship between Open Banking and Third-party Initiation?

The term "open banking" is used in different ways in different markets. In the European Union, the payment legislation (EU Directive 2015/2366) sets guidance on both account information and transaction data sharing with third parties, as well as payment initiation by third parties. Frameworks in Bahrain, Brazil, Japan, Singapore and the United Kingdom are similar.

In other markets, the topics may be separate. India's open banking regime focuses on data sharing only and makes no mention of payment initiation (RBI 2016). Open banking frameworks in Australia, HK, Malaysia and Mexico similarly do not introduce third-party payment initiation (Plaitakis and Staschen 2020). This does not mean that third party payment initiation does not exist in these markets, just that the conversation may be driven under a different banner (such as in India or Australia). Conversely, Indonesia's open banking standards cover payment initiation and not data sharing.[a]

a CGAP's own definition of open banking (Plaitakis and Staschen 2020) focuses on data sharing: "The exchange of consumer data between banks and other FSPs (i.e., data holders), on the basis of customer consent"

Box 3. Third-party initiation and financial inclusion—an ongoing debate

Critics are quick to point out that third-party initiation services are not doing the difficult work of bringing new customers into formal financial services (an existing financial account sits under each new third-party initiation), and they are typically not providing the cost and labor-intensive distribution networks (e.g., agents) necessary as the onramp between the cash and digital economies.

These points are true, but it is also clear that these services are improving the overall value proposition of financial accounts. The tremendous growth in transactions in a market like India shows that more informal economic activity is moving through formal channels than ever before.

In India, Google Pay has targeted kiranas (small merchants) through specific account features ('speech-to-text', use of 'Hinglish', credit, inventory, etc.) (Bhalla and Patwardhan 2021), and PhonePe announced in December 2021 having onboarded 25 million new small merchants in less than a year (TechCircle 2021). And in some cases these merchant services are also showing signs of beginning to expand cash-in-cash-out networks: PhonePe now allows customers to make cash out transactions at merchants who have enabled the PhonePe ATM feature.[a]

a Cash out through points of sales (POS) has been allowed by the RBI since 2009 for debit cards. The permission framework was extended to prepaid instruments in 2013. In 2020, the RBI waived the permission required for offering the service, and included all UPI transactions (see FAQ Cash Withdrawal Facility at POS).

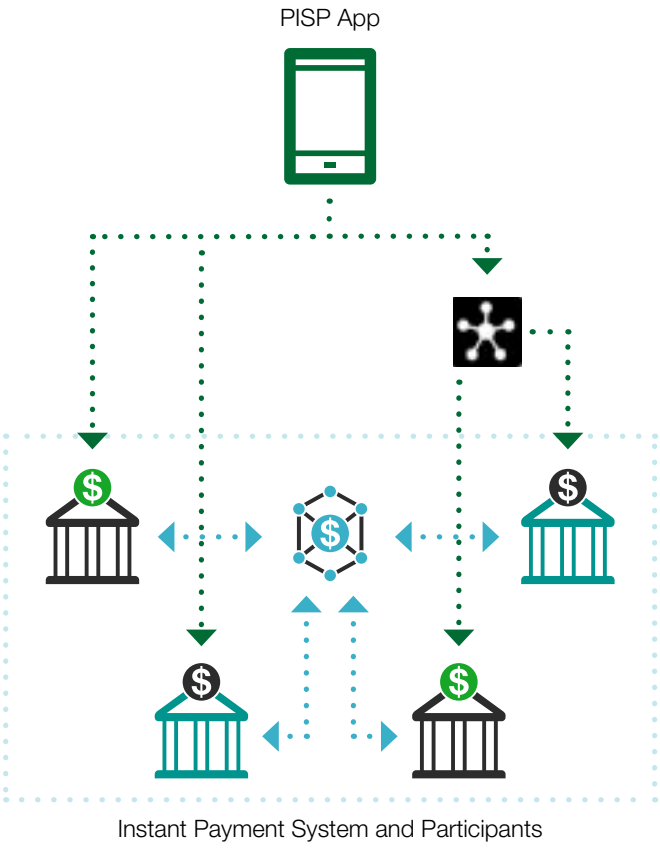
in their licensing framework for payments (e.g., the EU, Brazil), while in other markets these entities are not directly regulated unless they also offer a store of value (e.g., India).

Whatever the name, whatever the license, the concept is similar. Third-party initiation allows an entity other than the customer's account holder to initiate a transaction on behalf of the customer.

Decentralized model for third-party initiation

Some of the earliest examples of third-party initiation have applied a decentralized model for connecting PISPs to account-holding institutions. See Figure 10. In markets like the EU and UK, PISPs are linked through direct (or brokered) agreements to account-holding institutions, who in turn connect to the payment system.

FIGURE 10. **Decentralized model for third-party initiation**



In this model, the payment system does not play a direct role in passing initiation messages. Instead, PISPs bilaterally connect to APIs presented by account-holding institutions, who in turn initiate payments through the scheme as they would if no PISP were involved.

The advantage for the payment system operator is clear. The system is only serving in its role to pass payments between account-holding participants, and no additional investment, economic models, or changes to governance are required. PISP connectivity is instead left to the competitive space, with PISPs and a variety of other payment service providers (aggregators) forming direct business agreements to facilitate passing initiation messages.

However, there are challenges with this model. First, a system of bilateral and brokered connections for PISPs can result in a fragmented environment for payment initiation. A PISP app only works for a given account holder if the PISP has somehow connected with that institution. In small or highly concentrated banking markets, this may not be an issue. In markets with many account holders, or where those account holders serving poor people are at a competitive disadvantage in terms of technical capacity or negotiating power, this may be much more problematic.

Despite regulations mandating standard APIs for PISPs in both the EU and UK, the technical lift for integration can be substantial. Others argue that putting APIs in the competitive space has not served to improve service and lower costs (as was intended), but rather to reduce the efficiency of processes that could have been managed centrally at scale.

As a result, the market uptake for these models has been disappointing. In the UK, the number of active users accelerated during Covid-19, reaching 5 million by January 2022. This remains far behind the initial target of 33 million users by 2020.[6]

Centralized model for third-party initiation

Alternatively, a payment system can play a more direct role in brokering a PISP's connection to account-holding institutions. This simplifies some questions around issues like technical integration but raises a host of other questions in areas such as authentication, pricing models, and governance.

In India, PISP services have been centralized through UPI. While PISPs are not permitted to connect directly to UPI, UPI facilitates the exchange of information between account holders. In effect, banks act as a pass-through entity for the initiation of transactions by third parties. See Figure 11.

Fundamentally, requiring PISPs to connect to a payment system participant (rather than directly to the switch)

6 Initial estimates expected 33 million users of open banking by 2020, as shows the article "Lloyds Launches Open Banking App Feature", Pymnts.com (https://www.pymnts.com/pymnts-post/news/digital-banking/2019/lloyds-open-banking-app-halifax-barclays/?c=halifax#:~:text=Researchers%20say%20open%20banking%20services,five%20knew%20what%20it%20meant).

FIGURE 11. **Centralized (but brokered) model for third-party initiation**

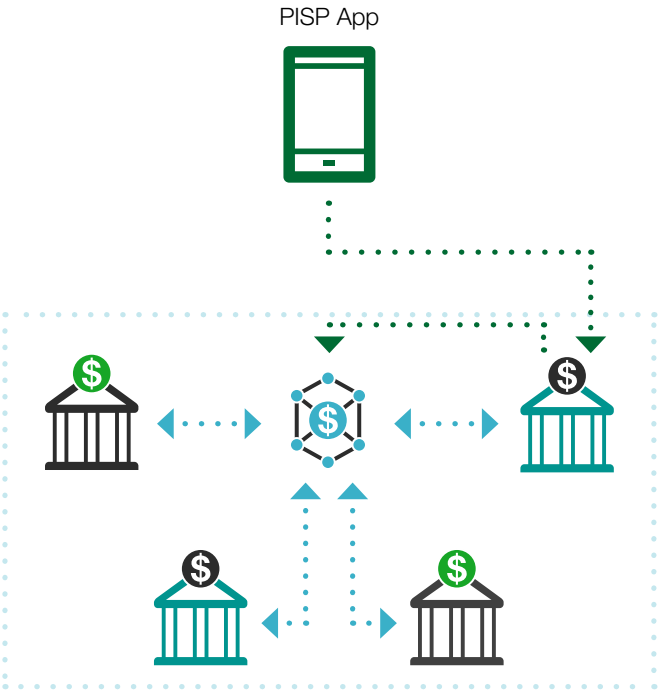
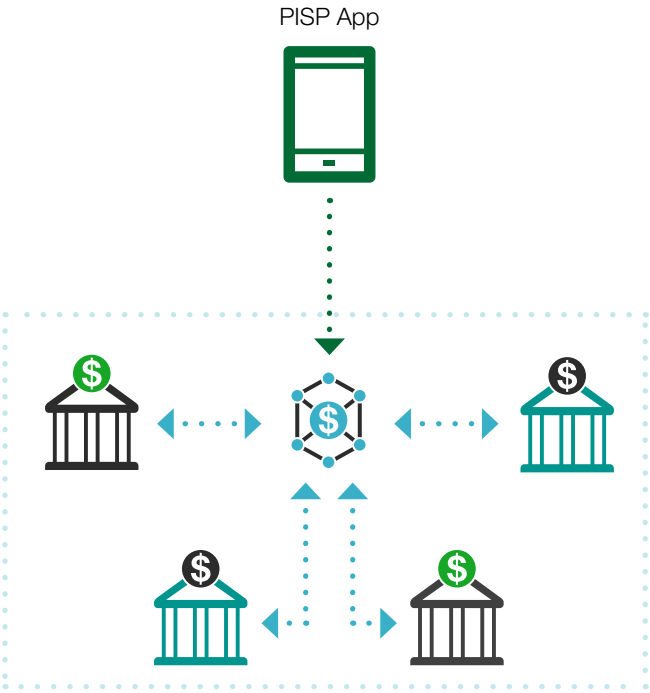


FIGURE 12. **Centralized (direct connection) model for third-party initiation**



is a risk decision. Remember that in India PISPs are not formally licensed and are therefore not held to the same regulatory requirements as direct UPI participants. A centralized but brokered model means that direct, account-holding participants retain responsibility for all transactions initiated through the switch.

However, as with most model choices in this paper, there is a tradeoff. Requiring PISPs to access the payment system through existing participants means they must enter one or more commercial agreements with banks or other payment system participants, forcing them to negotiate terms with potential competitors.

While there are fewer API connections required as compared to the decentralized model (e.g., UK and EU), most PISPs maintain more than one relationship for purposes of redundancy. In a well-publicized incident, India's PhonePe had operations stopped for 24 hours after its only partner bank, Yes Bank, was put under moratorium in March 2020. Google Pay, which at the time partnered with four banks, did not experience the same disruption (Ahmed 2020; Geewax 2021).

As shown in Figure 12, the alternative to a brokered connection to the payment system would involve a direct connection to the payment system operator, allowing a PISP to initiate transactions directly.

However, any form of centralized model (whether brokered or directly connected), raises a series of other questions for the scheme.

HOW WILL TRUST AND CONSENT PROCESSES BE MANAGED?

Any PISP arrangement must somehow establish trust across participants. Aida's bank knows her, and Aida's PISP knows her, but Aida's bank does not know that

Aida's PISP knows Aida. Where this shared trust does not exist, or cannot be adequately proven, risks emerge.[7]

For example, what is to prevent a PISP from simply sending money from Aida's account without her permission? How does her bank know that a message from the PISP is actually a message from Aida?

While these processes can be left to the private sector in a decentralized model (e.g., UK, EU), centralized models require the scheme to help answer them. There are two places where trust is needed in a third-party initiated transaction—account linking (i.e., when Aida pairs her PISP to her bank account) and the PISP-initiated transaction itself.

Establishing trust in the process of account linking isn't dissimilar to what one might experience in setting up an app or email account on a new device. Some type of token or electronic key can be provided to verify the user and establish a trusted link. This may require actions in both bank and PISP interfaces, but the challenges to the customer experience are hopefully limited in that it is a one-time action.

However, the question of trust becomes even more relevant to customer experience at the transaction level. In markets like the UK and EU, customers can be required to authorize each PISP transaction using their bank's interface. This involves the customer physically porting over to a separate app to finish a transaction started with the PISP. In a world where the intent of a PISP transaction is to free Aida from her bank's interface, this arrangement greatly diminishes the intended value of third-party initiation.

As an alternative, digital signatures and similar solutions can be used to allow transaction authorization to occur in the background. In India, UPI manages these authorization processes through API calls and responses between institutions. For each account that a user links to their UPI app they receive an MPIN from their bank, and these are stored in a secure NPCI utility. Authorization is managed between this embedded utility and the account holder via UPI, allowing the customer to complete the transaction without ever leaving the channel where the transaction started.

HOW WILL SCHEME ECONOMICS BE MANAGED?

Transaction switching costs are generally applied to the financial institutions that are debiting/crediting customer funds. It is conceivable that a payment system could charge PISPs some type of scheme fee for services provided. However, this has not been seen commonly in practice, and fees should be proportional to services where applied.

If a bank is brokering the PISP's connection to the switch, then the PISP and bank will likely enter a separate commercial agreement. In India, the large number of participating banks on UPI has prevented a scenario in which a PISP could be 'locked out' for failure to find a bank to contract.

In smaller or highly concentrated banking markets, it remains a risk that direct payment system participants could arrange through collusion or pricing to prevent indirect access to PISP services. The scheme and regulator should therefore monitor such relationships to help ensure a level playing field for service providers.

WHAT IS THE IMPACT FOR CUSTOMER PRICING?

Because a PISP transaction is also a transaction with the customer's account-holder, transaction fees from both entities can apply, layering the fee to the customer.

In a case like India, PISP payments can remain entirely free, regardless of the underlying bank, only because transaction fees are disallowed system-wide on UPI. The model has worked in India because most accounts are held by banks who earn revenue through intermediating funds rather than transaction fees. As PISP models become more prevalent in a wider diversity of markets (e.g., those

7 The Google paper *Design Principles for Third-Party Initiation* (Geewax 2021) discusses issues of trust and consent in detail, including specific recommendations for technical solutions that can be deployed by the payment system operator. However, it should be noted that this design guidance focuses on a centralized, non-brokered model for PISP connectivity, which Google advocates as best practice.

with MNO-led mobile money providers dependent on transaction fees), this poses greater challenges.

Pricing prohibitions (as in India) may appear to be a solution. However, such policies are also a high-risk strategy with potential unintended consequences for market development. In India, the RBI noted in a 2020 report that UPI pricing prohibitions were "impacting the survival of payment gateways, hampering innovation efforts and resulting in job losses and a slowdown in the expansion of the digital payment infrastructure" (RBI 2020).

At the same time, high fees imposed by banks at the account level have the potential to kill a PISP model before it has begun. As a result, the answer must be market- and context- specific. The best solution is likely when schemes/regulators focus on correcting specific market conduct issues, especially those related to price discrimination (e.g., when banks charge higher fees for PISP-initiated transactions than they would to the same customer for on-network transactions).

HOW WILL PISPs PARTICIPATE IN GOVERNANCE?

As non-account holders, PISPs are not involved in passing funds through the payment system, and so will typically not be considered full participants in the same way as banks or EMIs. However, PISPs are dependent on the scheme's services and have an impact on overall uptake in the market, so it is important that their voices are heard.

Scheme rules, including those on topics like data protection and cybersecurity, can also often apply (and should apply) to PISPs. Where PISPs are not direct participants or directly connected to the payment system, compliance with these requirements may be enforced through regulation or sponsoring banks.

Some schemes have found ways to account for the views of PISPs in payment system decision making. In Europe and the UK, PISPs are indirectly represented through payment associations such as the European Payment Institutions Federation (EPIF) and UK Finance. In Brazil, the regulator sets scheme rules, but hears input from an advisory committee that includes a wide range of actors, including PISPs.

REQUEST TO PAY

WHEN AIDA TOOK HER DEBIT card to the market in the earlier example, she only had to pass the merchant her card to begin the transaction. The merchant identified her address (the card number) and entered the amount on the Point-of-Sale (POS) device. Aida would still need to authorize the transaction, but the first step of the process asked little from her.

For an instant payment, Aida is required to do more work. She must enter the receiver's address and the amount she wants to send. She might get this information by scanning a QR code or by entering a till number, but in some way, she is responsible for obtaining and entering the necessary information. This presents a problem.

More responsibility on the customer means more room for error, especially for less digitally savvy users. Long queues, time pressure, noisy environments, and hard to read signs are just some of the things that can cause a customer to make errors with a payment.

Enter Request to Pay (RtP). RtP helps overcome these challenges by allowing a sender initiated (push) payment to look more like a receiver initiated (pull) payment. With an RtP transaction, the receiver begins the process by sending a secure message (literally, a request to pay) to the sender.

In line at the market, Aida is no longer expected to provide the merchant's address and the amount of the transaction. Like a card transaction, she only provides her own address to the merchant, perhaps showing her QR code. As shown in Figure 13, the merchant scans or enters the relevant information and sends a message, pre-filled with the details she needs in order to make a payment.

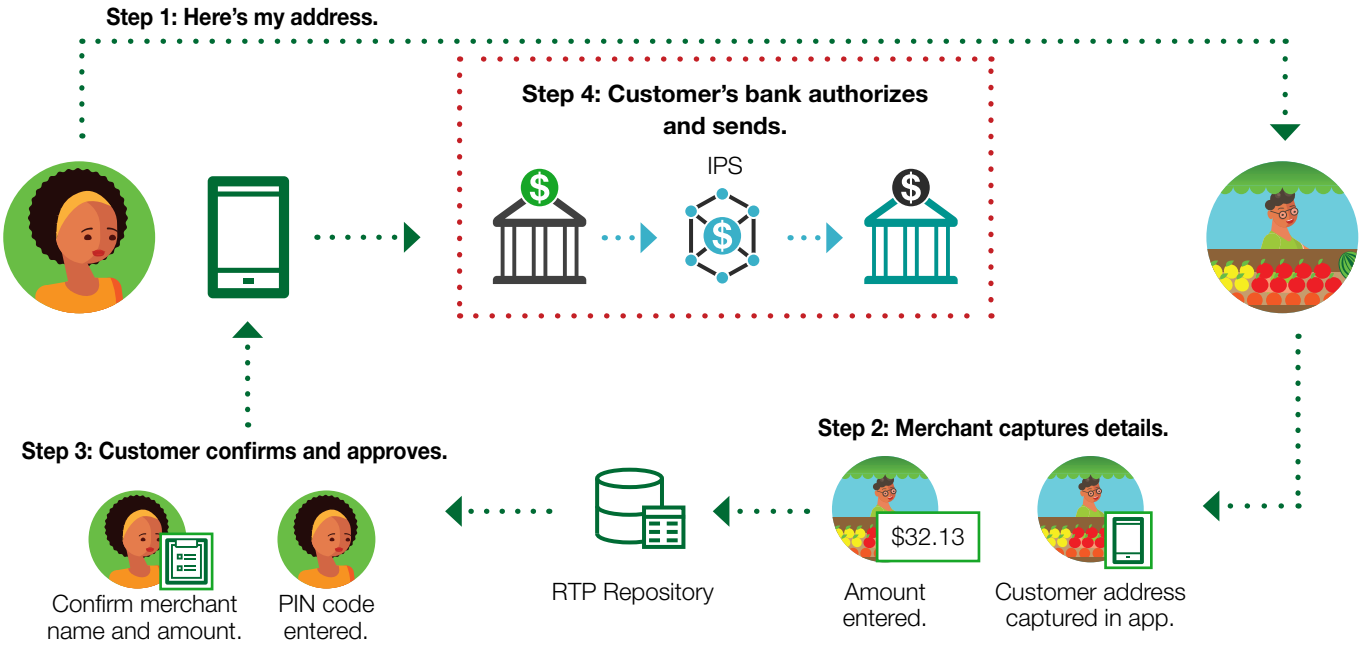
The Request to Pay service could be built into a merchant's point of sale device or app, or it could be provided by a separate third-party service. RtP service providers may connect directly or indirectly to the RtP service, which in turn may be enabled by private repositories (decentralized) or a single service offered by the scheme (centralized).

In markets like the UK, third-party acquirers such as Stripe offer RtP services to merchants via acquiring channels and also serve to host parts of the repository infrastructure. In markets like India, services are more centralized (Collect Requests by NPCI), but are similarly offered as an embedded service of merchant acquirers.

RtP should not be confused with the actual initiation of the payment. Aida is still initiating her own push-payment, the merchant is simply helping the process along—a bit like pre-filling a web form in the world of e-commerce. Aida gets some of the benefits of a card experience, and our grocer can be confident that the address and amount information are correct.

RtP services are still emerging around the world. Mexico's CoDi, India's UPI RtP service, called Collect Requests, and Australia's PayTo service are three early examples. However, numerous others are being formed, including those supporting instant payment systems in developed markets such as the European Union, the UK and the US.

FIGURE 13. **Request to Pay transaction**



Design Considerations

As compared to third-party payment initiation, design questions related to Request to Pay are more straightforward. Request to Pay is fundamentally a messaging service operating outside the walls of the trust/consent framework necessary for transaction authorization. Once Aida receives a Request to Pay, she still needs to authorize the transaction (whether through her bank or a PISP).

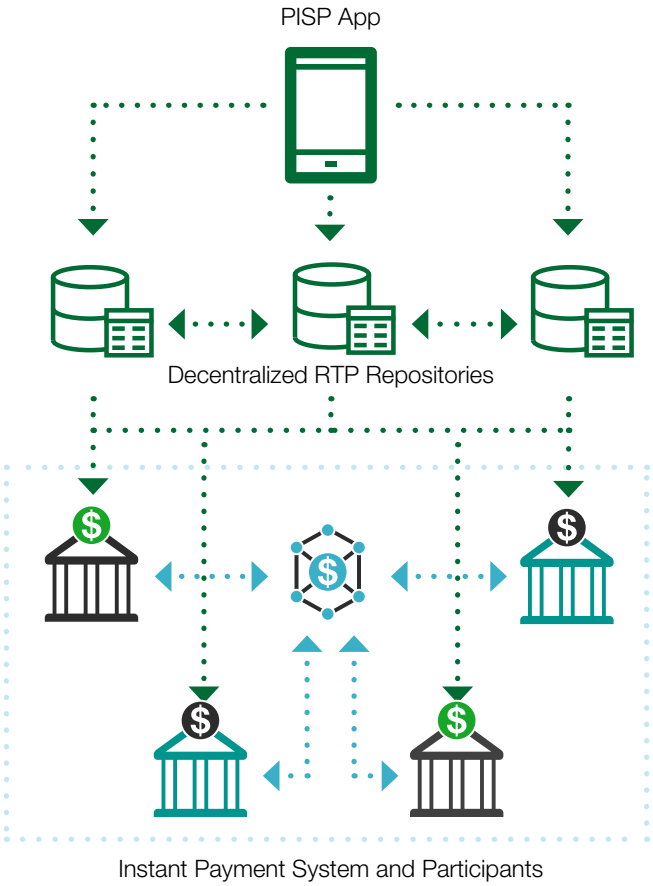
Similar to their approach to PISP services, the UK and EU have applied a decentralized approach to Request to Pay. (See Figure 14).

The payment system does not play a role in passing these requests. Connections between RtP providers and account issuers are managed through a series of bilateral connections. And the economics are largely left to the private sector.

However, a few key differences exist. Because RtP does not involve payment initiation, issues of trust and consent become less critical. The operational framework can be lighter, and more open architectures are possible.

The UK's RTP service uses messaging built on the same open messaging standards used for email, with internet

FIGURE 14. **Decentralized model for Request to Pay**



DNS servers used to find the RtP message recipient's address. Initially, these addresses will be domain-based in the UK (similar to the VPA directory for UPI in India), but eventually users will be able to register their existing email address or other alias.

Pay.UK, the same entity that administers the Faster Payments scheme, sets the standards (e.g., user experiences, messaging frameworks) and provides certification for repository and application providers. Pay.UK convenes an RtP Development Group where repository and app providers have the chance to provide input on the RtP Framework and technical standards. However, private actors operate the repositories (route and store messages) and applications (view and send requests).

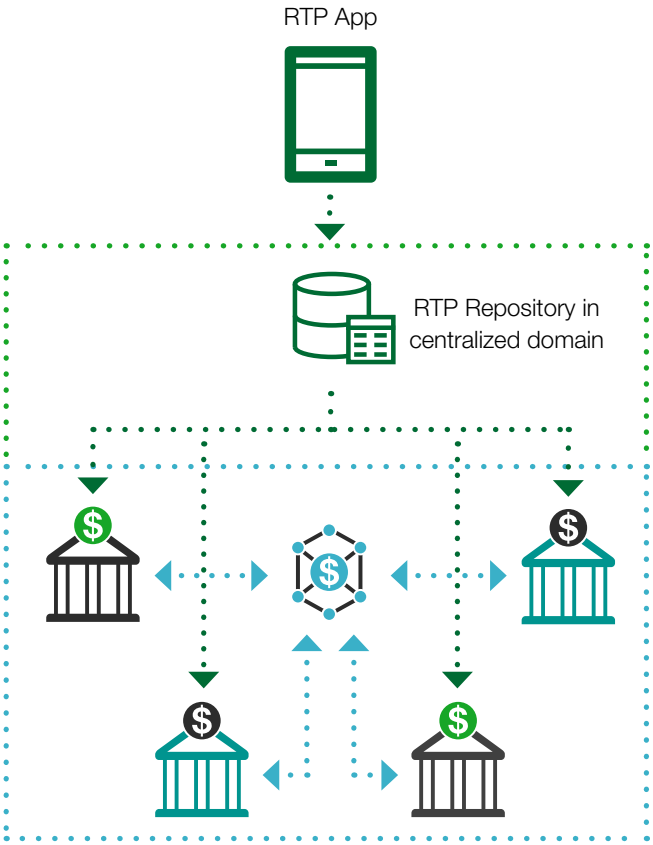
Pay.UK charges a very small fee to repositories (0.0075 of a Penny for each successful end-to-end RtP message), which in turn may charge app providers for the service. Application providers may charge the customer or include RtP as a value-added service to existing acquiring businesses. A single provider (e.g., Mastercard) may opt to combine both roles and commercial models.

Countries including India (Collect Requests) and Mexico (CoDi) have implemented Request to Pay solutions built on a more centralized model. (See Figure 15). The RtP app (again either provided by existing acquirers or third parties, as approved by the regulator) will connect to the RtP repository which routes the request to the payer. The key difference here from the UK model described above is that the RtP repository in the centralized model may use the same address resolution database as the payment system and end users need not register separately for RtP.

In a centralized approach, the RtP app providers are likely to adopt a value-added service approach. The repository, rather than being left in the competitive domain, becomes a shared utility at the market/scheme level.

While comparatively lower risk than payment initiation services, consumer protections remain important, regardless of the operational model pursued. Designing RtP with these protections in mind helps prevent fraud, especially for vulnerable customers, but also helps to limit transaction disputes. Examples of protections include:

FIGURE 15. **Centralized model for Request to Pay**



- Requesting expiration after a certain period of time (e.g., two days in India), to help prevent erroneous payment of a cancelled/aborted transaction
- Verified merchant programs to help avoid the risk of fraudulent payment requests through phishing and similar threats
- Limits on the ability for the request receiver to modify variables of a request before payment (e.g., instead submitting a change request to the merchant via RtP channel)

Sharing more than payments (RtP and value-added services)

RtP services are also increasingly supporting other value-added services beyond payment transaction information. (See Figure 16). Some examples include:

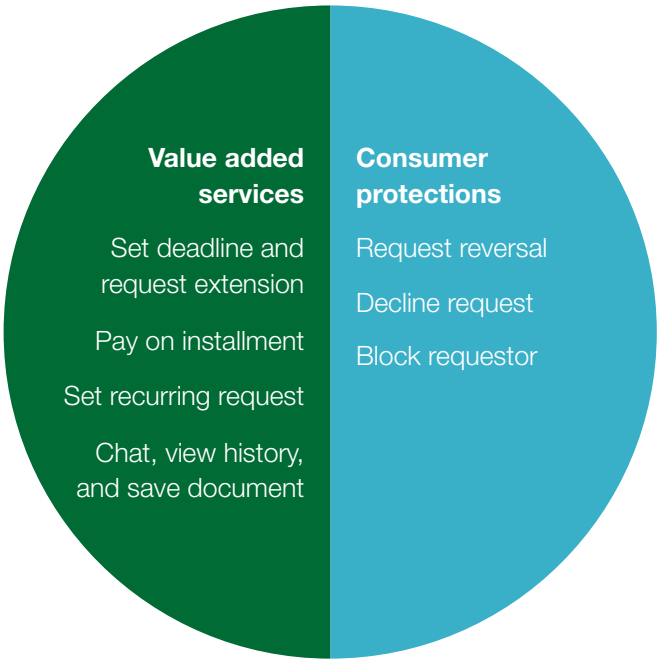
- **Payment deadlines and extension requests** – Both Pay.UK and SEPA RtP in the EU have introduced the ability for the receiver to set a payment deadline, and for the sender to ask for more time to pay. These features are particularly relevant for bill payments and remote transactions (Pay.uk 2022).
- **Pay part of the transaction, or request installment payments** – RtP in the UK also allows senders the option to pay only a part of the transaction. A proposed change in 2021 for SEPA's RtP may take this a step further to allow for installment payments (EPC 2022).
- **Setting recurring requests** – Some RtP services are offering recurring requests. Again, this is a feature particularly relevant for bill payment. Examples can be found in the implementations of RtP in UK, Australia and India.

Taking RtP's capability for richer transaction detail even a step further, some services are now allowing payors to **view request history, chat with biller, or allow documents (such as an invoice) to be attached.** This enhanced level of data has the potential to allow customers to store payment information for personal or tax-management purposes.

As with any financial product, security, data protection, and resilience must also be priorities. Today's RtP services commonly build in redundancies for communications delays/failures and security functions such as message duplication checks. For the sender, features such as **declining the request** and **blocking the requestor** are also common.

Another benefit of RtP services is that they may be used to **request the return** of an amount where a payment has been made in error. Instant payments are often irrevocable, meaning that schemes do not facilitate transaction reversal in the same way as for card payments (i.e., the liability rests instead with the customer). RtP solutions can help to bridge this gap, providing a way for customers to interact directly with merchants on disputes.

FIGURE 16. **Examples of additional functionality in Request to Pay infrastructure**



SCHEMES AND CUSTOMER EXPERIENCE – WHERE TO DRAW THE LINE?

CUSTOMER EXPERIENCE MATTERS, as evidenced by the fact that more than 80% of UPI transactions in India are initiated by non-account holding institutions (NPCI 2021). Similarly, 17 million previously dormant bank account holders in Brazil made their first digital payment following the launch of Pix (BCB 2021, p.127). Customer experience is important to the value proposition of instant payments, but it is also fundamental to the private sector's ability to differentiate its products and compete in the market.

Where should a scheme draw the line between facilitating market competition and collaboration?

Any interoperability arrangement balances competition and collaboration among participants. Competitors are choosing to work together to increase overall value to the market. But this value can also be undermined if a scheme interferes too much in defining the product, limiting the ability of actors in the private sector to stand apart from their competitors.

Some schemes have recognized that lower capacity institutions—particularly those such as microfinance institutions which disproportionately serve poor people—may not be able to deliver on best-in-class user experience. As a result, they have taken the step to provide tools to help participants drive better customer service (e.g., the BHIM app by NPCI in India).

While India's BHIM app has been largely successful, other similar efforts have met with mixed results. CoDi in Mexico offers a generic RtP app for participants, yet some hurdles exist in the customer experience (e.g., users port to bank app to authorize transaction), and CoDi uptake remains limited (CoDi 2022). In Nigeria, NIBSS launched mCash, a USSD product designed to initiate merchant payments from any account, but uptake was slow as banks preferred to champion their own products (TechPoint.africa 2018).

Where these efforts succeed some common traits are observed:

1. A focus on enablement over requirement. Rather than requiring use by participants, they are available as tools for those who need them (leaving those who want to invest in their own solutions free to do so).
2. Best-in-class solutions, meeting private sector demands. To truly act as a tool for market enablement, a solution offered by the scheme must be better than what is already available to participants and in line with the market's strategic priorities.

In India, NPCI worked with the open-source developer community iSPIRT to develop the BHIM app. BHIM was successful in part because it was well designed. In an independent design review of six financial services apps, BHIM emerged with top honors (Raman and White 2017). Yet even here, BHIM triggered concerns in some corners that NPCI was acting simultaneously as scheme-owner, standard-setter, and solution-developer—an arrangement with potentially negative effects on market competition.

REFERENCES

Ahmed, Shehnaz. 2020. "Yes Bank Collapse Exposes the Fault-Lines in India's Fintech Industry". Vidhi Center for Legal Policy. March 23, 2020. https://vidhilegalpolicy.in/blog/yes-bank-collapse-exposes-the-fault-lines-in-indias-fintech-industry/.

Banco Central do Brasil (BCB). 2021. *Relatório de Cidadania Financeira.* https://www.bcb.gov.br/content/cidadaniafinanceira/documentos_cidadania/RIF/Relatorio_de_Cidadania_Financeira_2021.pdf.

Bhalla and Patwardhan. 2021. "Google Pay bets on voice-led payments, drives kirana play". *Mint,* November 19, 2021. https://www.livemint.com/companies/news/google-pay-bets-on-voice-kirana-tech-in-india-11637234009001.html.

CoDi. 2022. *Estatistícas de la plataforma CoDi.* Accessed on September 13, 2022. https://www.codi.org.mx/paginas/Estadisticas.html.

Collie, Vaughan, Anant Nautiyal, Akihiro Ishizuka, Bart-Jan Pors, Bruno Martins, Jannen Vamadeva. 2020. "QR Code Merchant Payments ». *Inclusive Tech Lab.* GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/08/QR-Code-Merchant-Payments-A-growth-opportunity-for-mobile-money-providers-incl-full-appendices.pdf.

Cook, William, Dylan Lennox and Souraya Sbeih. 2021. *Building Faster Better: A Guide to Inclusive Instant Payment Systems.* CGAP. https://www.cgap.org/research/publication/building-faster-better-guide-inclusive-instant-payment-systems.

EU Directive 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.

European Payments Council (EPC). 2022. *SEPA Request-to-Pay Scheme Rulebook, 2022 Change Request Public Consultation Document.* EPC074-22 / Version 1.0. https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-05/EPC074-22%20v1.0%20SRTP%20Scheme%20Rulebook%202022%20Change%20Request%20Public%20Consultation%20Document.pdf.

Geewax, JJ. 2021. *Design Principles for Third-party Initiation in Real-time Payment Systems.* Google. https://research.google/pubs/pub50087/.

National Payments Corporation of India (NPCI). 2021. "Standard Operating Procedure (SOP) – Market Share Cap for Third Party Application Service Providers (TPAP)". NPCI/UPI/SOP-01/2020-21. https://www.npci.org.in/PDF/npci/upi/circular/2021/standard-operating-procedure-sop–market-share-cap-for-third-party-application-providers-tpap.pdf.

Open Banking. 2022. "Open Banking passes the 5 million users milestone". Accessed on September 13, 2022. https://www.openbanking.org.uk/news/open-banking-passes-the-5-million-users-milestone/.

Pay.UK. 2022. "Request to Pay." Accessed on September 13, 2022. https://www.wearepay.uk/programmes/end-user-deliverables/request-to-pay/.

Plaitakis, Ariadne and Stefan Staschen. 2020. *Open Banking: How to Design for Financial Inclusion.* CGAP. https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Open_Banking.pdf.

Raman, Anand, and Gabriel White. 2017. "Financial Services Apps in India: How to Improve User Experience." CGAP. https://www.cgap.org/sites/default/files/publications/slidedeck/Financial-Services-Apps-in-India-Mar-2017.pdf.

Reserve Bank of India (RBI). 2020. *Report of the Committee on the Analysis of QR (Quick Response) Code.* https://www.wearepay.uk/programmes/end-user-deliverables/request-to-pay/.

Reserve Bank of India (RBI). 2016. *Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions*. RBI/DNBR/2016-17/46, Master Direction DNBR.PD.009/03.10.119/2016-17. https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

Sendingan, Sandra. 2019. "Singapore rolls out world's first unified payment QR code". *Asian Banking and Finance.* https://asianbankingandfinance.net/cards-payments/news/singapore-rolls-out-worlds-first-unified-payment-qr-code.

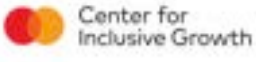
TechCircle. 2021. "PhonePe acquires 25mn new merchants, kirana stores in less than a year". *TechCircle,* December 13, 2021. https://www.techcircle.in/2021/12/13/phonepe-digitises-25-mn-small-merchants-kirana-stores-across-india.

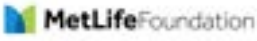
TechPoint.africa. 2018. "4 reasons mCash never really caught on". *TechPoint.africa,* August 9, 2018. https://techpoint.africa/2018/08/09/4-reasons-mcash-never-really-caught-on/.

Venkatanarayanan, Anand and Srikanth Lakshmanan. 2017. "Aadhaar Mess: How Airtel Pulled Off Its Rs 190 Crore Magic Trick". *The Wire*, December 21, 2017. https://thewire.in/banking/airtel-aadhaar-uidai.










CGAP members as of February 2023


CGAP
cgap.org